

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TEXAS  
MIDLAND-ODESSA DIVISION**

**Malikie Innovations Ltd. and  
Key Patent Innovations Ltd.,**

**Plaintiffs,**

**v.**

**MARA Holdings, Inc. (f/k/a Marathon  
Digital Holdings, Inc.)**

**Defendant.**

§  
§  
§  
§  
§  
§  
§  
§  
§  
§

**Case No. 7:25-cv-00222-DC-DTG**

**JURY TRIAL DEMANDED**

**FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT  
AND JURY DEMAND**

Plaintiffs Malikie Innovations Ltd. (“Malikie”) and Key Patent Innovations Ltd. (“KPI”) (collectively, “Plaintiffs”), by and through their undersigned counsel, bring this First Amended Complaint for patent infringement and damages against Defendant MARA Holdings, Inc. (f/k/a Marathon Digital Holdings, Inc.) (“MARA” or “Defendant”) and, in support, allege the following:

**PARTIES**

1. Plaintiff Malikie is the successor-in-interest to a substantial patent portfolio created and procured over many years by Blackberry Ltd., formerly known as Research in Motion Ltd., and its predecessor, subsidiary, and affiliated companies (collectively, “Blackberry”). Malikie is an Irish entity duly organized and existing under the laws of Ireland. Malikie has registered offices at: The Glasshouses GH2, 92 Georges Street Lower, Dun Laoghaire, Dublin A96 VR66, Ireland.

2. Plaintiff KPI is the beneficiary of a trust pursuant to which Malikie owns, holds, and asserts the Asserted Patents (set forth below). KPI is an Irish entity duly organized and existing under the laws of Ireland. KPI has registered offices at: The Glasshouses GH2, 92 Georges Street Lower, Dun Laoghaire, Dublin A96 VR66, Ireland.

3. On information and belief, Defendant MARA Holdings, Inc. (“MARA”), formerly known as Marathon Digital Holdings, Inc., is a Nevada corporation, with a principal place of business at: 101 NE Third Avenue, Suite 1200, Fort Lauderdale, FL. On information and belief, MARA maintains operational facilities in Texas, including in this District, and in other states. On information and belief, MARA owns and operates the website located at [www.mara.com](http://www.mara.com).<sup>1</sup>

### **NATURE OF THE ACTION**

4. This is a civil action for patent infringement under the patent laws of the United States, 35 U.S.C. § 1 *et seq.*

5. This case centers on ground-breaking innovations in elliptic curve cryptography that were discovered by some of the field’s leading technologists at Certicom Corporation and Blackberry Limited (formerly known as Research In Motion, or “RIM”), that years later were recognized and selected by the designers of Bitcoin<sup>2</sup>— far and away the world’s most valuable cryptocurrency—to enable Bitcoin’s characteristic quality as a “trustless” payment system requiring no third party intermediary. Specifically, the Bitcoin protocol incorporates cryptographic technology developed and patented by Certicom and Blackberry—technology covered by the Asserted Patents. Defendant, in turn, uses this patented technology to operate one of the largest bitcoin mining operations in the world, manage its proceeds, and engage in bitcoin transactions.

6. Malikie is the assignee of and owns all right and title to U.S. Patent Nos. 8,788,827 (the “’827 Patent”); 10,284,370 (the “’370 Patent”); 8,666,062 (the ’062 Patent”); 7,372,960 (the “’960 patent”); 7,372,961 (the “’961 patent”); and 8,532,286 (the “’286 Patent”) (collectively, the

---

<sup>1</sup> All URLs cited herein were last visited on April 28, 2025, unless otherwise noted.

<sup>2</sup> As used herein, “Bitcoin” with a capital “B” refers to Bitcoin’s protocol, network, and blockchain, whereas “bitcoin” with a lower case “b” refers to the unit of cryptocurrency.

“Asserted Patents”), which were duly and legally issued by the United States Patent and Trademark Office (“USPTO”). Malikie seeks monetary damages and, where appropriate, injunctive relief.

## **FACTS COMMON TO ALL CLAIMS**

### **Background**

#### ***The Rise of Bitcoin***

7. Earlier this year, the price of a single bitcoin (1 BTC<sup>3</sup>) reached \$109,000.<sup>4</sup> While that is an impressive figure in absolute terms, it is even more impressive considering how much the value of bitcoin has increased over the years. When today’s leading U.S.-based cryptocurrency exchange was founded in 2012, “a bitcoin was worth \$6 and only known by a few nerds on the internet.”<sup>5</sup> Just two years prior to that, 1 BTC was worth less than a penny: \$0.0041. On May 22, 2010, in what is widely understood to be the first commercial Bitcoin transaction, Laszlo Hanyecz (one of Bitcoin’s earliest developers and proponents) paid 10,000 BTC—worth about \$41 at the time—for two Papa John’s pizzas.<sup>6</sup> And only seven months before that, 1 BTC was worth just \$0.00099. In the first ever exchange of bitcoin for U.S. dollars, Marti Malmi (Bitcoin’s second developer after Satoshi Nakamoto) sold 5,050 BTC for \$5.02 on October 12, 2009.<sup>7</sup> Following the meteoric rise of Bitcoin, had they kept them, Hanyecz’s 10,000 BTC would have been worth over \$1 billion in January 2025 and Malmi’s 5,050 BTC would have been worth over \$550 million. No other cryptocurrency has attained such incredible value.

---

<sup>3</sup> “BTC” is a common unit used to designate one bitcoin. See <https://bitcoin.org/en/vocabulary#btc>. Bitcoin can be transacted in units smaller than 1 BTC, in units of “satoshi,” which is the smallest unit of bitcoin, equivalent to a one hundred millionth of a single bitcoin (0.00000001 BTC). See [https://en.bitcoin.it/wiki/Satoshi\\_\(unit\)](https://en.bitcoin.it/wiki/Satoshi_(unit)).

<sup>4</sup> <https://www.coinbase.com/price/bitcoin>.

<sup>5</sup> <https://www.cnbc.com/2021/04/14/coinbase-co-founders-launched-when-a-bitcoin-btc-was-worth-6.html> (quoting Fred Ehrsam, co-founder of Coinbase).

<sup>6</sup> <https://www.youtube.com/watch?v=tWU3O3X5kKE>; <https://www.coinbase.com/learn/crypto-glossary/what-is-bitcoin-pizza>.

<sup>7</sup> <https://bitcoinmagazine.com/markets/bitcoins-first-trade-now-worth-130-million>.

8. Bitcoin is regarded as the first “cryptocurrency” and “remains by far the biggest, most influential, and best-known.”<sup>8</sup> Other leading cryptocurrencies today include Ethereum, Tether, and Solana, which, although they are perhaps relatively well-known among those familiar with cryptocurrency, are worth orders of magnitude less than Bitcoin.<sup>9</sup> Thousands of cryptocurrencies exist today<sup>10</sup>, but, as the Ethereum website acknowledges, “[i]t all started with bitcoin.”<sup>11</sup>

9. While Bitcoin is the foundation of today’s sprawling cryptocurrency market, the foundation of Bitcoin’s trailblazing trustless digital currency model—its digital signature framework—uses cryptographic technology developed and patented by Certicom and Blackberry.<sup>12</sup> Bitcoin’s adoption of this technology set a trend that has propagated throughout the cryptocurrency landscape.

### ***Bitcoin’s Foundation on Certicom-Developed Cryptography***

10. The creation of Bitcoin is attributed to Satoshi Nakamoto (“Satoshi”), the presumed pseudonym used by the author<sup>13</sup> of a white paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System,” which was reportedly sent on October 31, 2008 to a small group of recipients on “The Cryptography Mailing List” using a pipermail message service hosted by metzdowd.com.<sup>14</sup> Satoshi’s message included a link to the white paper, which was (and still is) hosted at bitcoin.org,

---

<sup>8</sup> <https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency>.

<sup>9</sup> See, e.g., *id.*; <https://coinmarketcap.com/>.

<sup>10</sup> For example, the Coinbase exchange lists hundreds of tradable crypto assets among thousands in existence. <https://www.coinbase.com/explore>.

<sup>11</sup> <https://ethereum.org/en/what-is-ethereum/> (answering “What is a cryptocurrency?”).

<sup>12</sup> <https://bitcoin.org/bitcoin.pdf> (“Bitcoin Whitepaper”) at 1, 2, 8.

<sup>13</sup> Satoshi Nakamoto might be one or more persons. See, e.g., <https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html> (“I’ve been working on a new electronic cash system...”); *id.* (“We propose a solution to the double spending problem...”).

<sup>14</sup> See Bitcoin Whitepaper; see also <https://www.wired.com/story/after-10-years-bitcoin-changed-everything-nothing/>.

a site “originally registered and owned by Bitcoin’s first two developers, Satoshi Nakamoto and Martti Malmi.”<sup>15</sup>

11. The first line of Satoshi’s initial message to the “cryptography” community articulated the goal of Bitcoin: to provide “a new electronic cash system that’s fully peer-to-peer, with no trusted third party.”<sup>16</sup> This defining characteristic of Bitcoin is achieved using cryptography.<sup>17</sup> Specifically, “[d]igital signatures provide part of the solution.”<sup>18</sup> As Satoshi explained in a February 11, 2009 message to another online community—the “p2p-research” mailing list—“[o]ne of the fundamental building blocks for such a system [as Bitcoin] is digital signatures.”<sup>19</sup>

12. A digital signature is a cryptographic tool for verifying the authenticity of digital data (*i.e.*, validating its original source and genuineness) and its integrity (*i.e.*, that it is accurate, complete, and has not been tampered with).<sup>20</sup> In fact, a bitcoin is fundamentally just “a chain of digital signatures” recorded in a public history or “chain” of transactions. *See* Bitcoin Whitepaper at 2 (“We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin.”), 8 (describing “a peer-to-peer network using proof-of-work to record a public history of transactions”).

---

<sup>15</sup> <https://bitcoin.org/en/about-us#own>; <https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html>.

<sup>16</sup> <https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html>; *see also* Bitcoin Whitepaper (abstract).

<sup>17</sup> Bitcoin Whitepaper at 1 (“What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”).

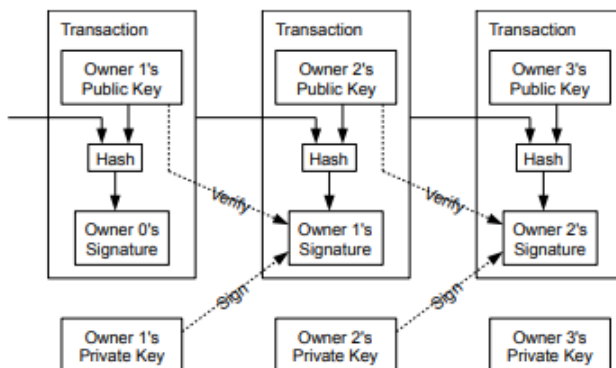
<sup>18</sup> <https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html> (abstract); Bitcoin Whitepaper (abstract).

<sup>19</sup> <https://satoshi.nakamotoinstitute.org/emails/p2p-research/35/>.

<sup>20</sup> <https://www.cisa.gov/news-events/news/understanding-digital-signatures>.

## 2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



Bitcoin Whitepaper at 2

See also <https://satoshi.nakamotoinstitute.org/emails/p2p-research/35/> (“A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership”). Specifically, as Satoshi explained to the “cryptography” community shortly after releasing the white paper but before releasing the first version of Bitcoin software, “it’s ECC digital signatures.”<sup>21</sup>

13. The acronym “ECC” stands for elliptic curve cryptography.<sup>22</sup> ECC “represents a different way to do public-key cryptography—an alternative to the older RSA system—and also offers certain advantages.”<sup>23</sup> “ECC devices require less storage, less power, less memory, and less bandwidth than other systems. This allows you to implement cryptography in platforms that are constrained, such as wireless devices, handheld computers, smart cards, and thin-clients. It also provides a big win in situations where efficiency is important.”<sup>24</sup> As explained by Certicom

<sup>21</sup> <https://satoshi.nakamotoinstitute.org/emails/cryptography/14/>; see also <https://satoshi.nakamotoinstitute.org/emails/cryptography/2/> (explaining that “ECC is nicely compact”).

<sup>22</sup> [https://en.bitcoin.it/wiki/Elliptic\\_curve\\_cryptography](https://en.bitcoin.it/wiki/Elliptic_curve_cryptography).

<sup>23</sup> <https://www.certicom.com/content/certicom/en/the-basics-of-ecc.html>.

<sup>24</sup> *Id.*

Corporation, “the authority for strong, efficient cryptography,” when asymmetric cryptography (such as public-key cryptography) is desired “Elliptic curve cryptography (ECC) is the best choice, because” it “will give you the most security per bit.”<sup>25</sup> For example, “ECC offers considerably greater security for a given key size” and enables “faster cryptographic operations, running on smaller chips or more compact software” resulting in “less heat production and less power consumption.”<sup>26</sup>

14. ECC is also secure. In 1997, Certicom introduced the “Elliptic Curve Cryptosystem (ECC) Challenge” as a way “to increase industry understanding and appreciation for the difficulty of the elliptic curve discrete logarithm problem, and to encourage and stimulate further research in the security analysis of elliptic curve cryptosystems.”<sup>27</sup> Certicom challenged participants to compute the ECC private key from a list of ECC public keys and associated parameters.<sup>28</sup> The challenge included relatively easier (Level I) challenges, some of which have been solved, and more difficult (Level II) challenges, which Certicom believed to be “computationally infeasible” and still have not been solved.<sup>29</sup>

15. As mentioned above, Bitcoin uses ECC digital signatures. Specifically, Bitcoin uses an elliptic curve digital signature algorithm (“ECDSA”) with parameters known as “secp256k1.”<sup>30</sup> Secp256k1 is defined in a Standards for Efficient Cryptography (SEC) specification titled “SEC 2: Recommended Elliptic Curve Domain Parameters” (Version 2.0, Jan.

---

<sup>25</sup> <https://www.certicom.com/content/dam/certicom/images/pdfs/WP-ECCprimer.pdf> at 3, 22.

<sup>26</sup> *Id.* at 3.

<sup>27</sup> <https://www.certicom.com/content/certicom/en/the-certicom-ecc-challenge.html>.

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*

<sup>30</sup> [https://en.bitcoin.it/wiki/Elliptic\\_Curve\\_Digital\\_Signature\\_Algorithm](https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm); <https://en.bitcoin.it/wiki/Secp256k1>.

2010), which is a publication of the Standards for Efficient Cryptography Group (SECG).<sup>31</sup> The SEC 2 paper (Version 2.0) was generated by Certicom Research and identifies Dan Brown of Certicom as the main contact.<sup>32</sup> Dan Brown is a co-inventor of several of the Asserted Patents in this case. *See infra*.

16. Certicom—which was “[f]ounded in 1985, the same year Elliptic Curve Cryptography (ECC) was invented”—has a long been regarded as the leader in ECC technology.<sup>33</sup> Indeed, Scott Vanstone, who co-founded Certicom in 1985 with Gord Agnew and Ron Mullin, was an internationally recognized top ECC researcher and the recipient of prestigious awards and recognitions for his monumental and profound contributions in the field of ECC.<sup>34</sup> Vanstone authored numerous papers and was awarded hundreds of patents related to ECC.<sup>35</sup> To help drive ECC’s commercial adoption, Certicom (with Vanstone) founded the SECG in 1998.<sup>36</sup> The purpose of the SECG is “to develop commercial standards that facilitate the adoption of efficient cryptography and interoperability across a wide range of computing platforms.”<sup>37</sup> “SECG members include leading technology companies and key industry players in the information security industry,” including its founding member, Certicom.<sup>38</sup> Certicom’s development of a standards body to promote ECC was welcomed by many in the cryptography industry. As the

---

<sup>31</sup> <https://www.secg.org/sec2-v2.pdf> at 9.

<sup>32</sup> *Id.* (cover page).

<sup>33</sup> <https://www.certicom.com/content/certicom/en/about.html>.

<sup>34</sup> *See, e.g.*, <https://www.certicom.com/content/certicom/en/about/news/release/2004/certicom-founder-scott-vanstone-wins-prestigious-research-award.html>; <https://www.certicom.com/content/certicom/en/about/news/release/2009/certicom-founder-wins-premiers-catalyst-award-for-lifetime-achieve.html>; <https://uwaterloo.ca/news/profound-impact-researcher>.

<sup>35</sup> *See id.*

<sup>36</sup> <https://www.cnet.com/tech/tech-industry/certicom-creates-standards-body/>.

<sup>37</sup> <https://www.secg.org/>.

<sup>38</sup> *Id.*; *see also* <https://www.certicom.com/content/certicom/en/about/news/release/2005/standards-for-efficient-cryptography-group--secg--announce-new-i.html> (identifying Certicom as “a founding member of SECG”).



chief scientist of one security firm put it in 1998, “It’s good news for the industry as a whole to move ECC forward because it is a promising technology.”<sup>39</sup> In 2004, a professor at Texas Tech University (winner of the Certicom Elliptic Curve Cryptography (ECC)2-109 Challenge) said, “I think public-key cryptography based on ECC is what we should and will be moving toward.”<sup>40</sup> Walt Davis, former senior vice-president at Motorola, told Vanstone that he believed “ECC was the only technology that would work in their constrained environments.”<sup>41</sup>

17. Demonstrating its position as the leader in developing and promoting ECC technology, Certicom hosted the annual ECC Conference beginning in 2004, which “was designed to interest both a technical audience and business managers.”<sup>42</sup> Vanstone recalled that the 2004 conference “was well-attended by cryptography experts, industry leaders and members of the developer community.”<sup>43</sup> The conference also “held significant historical value,” with “luminaries such as Dr. Ralph Merkle, Dr. Neal Koblitz, Dr. Victor Miller and Dr. Walt Davis” in attendance.<sup>44</sup> Those luminaries were the pioneers of public key cryptography and ECC: Miller and Koblitz “independently invented elliptic curve cryptography”; Merkle was one of the inventors of public key cryptography; and Davis was a senior vice-president at Motorola who was an early advocate for ECC and recipient of the first ECC Visionary Award.<sup>45</sup> As a testament to Certicom’s status as the unrivaled leader and authority in ECC research and development, industry members recognized that “[t]he one thing holding up elliptic curve cryptography is standards,” and that “Certicom is

---

<sup>39</sup> <https://www.cnet.com/tech/tech-industry/certicom-creates-standards-body/>.

<sup>40</sup> <https://www.metzdowd.com/pipermail/cryptography/2004-April/006798.html>.

<sup>41</sup> <https://www.certicom.com/content/certicom/en/code-and-cipher/article/529-reflections-the-year-that-was-.html>.

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

the only firm that could drive a standards effort, since it is the most commercial promoter of elliptic curve crypto.”<sup>46</sup> Indeed, Certicom has been described as the “authority,” “leader,” and “expert” in the field of ECC.<sup>47</sup>

18. Resulting from its pioneering discoveries in ECC, Certicom is well known to have been the holder of many valuable patents covering certain implementations of ECC. For example, Bruce Schneier<sup>48</sup>, an internationally renowned security technologist (known as the “security guru”) and Adjunct Lecturer in Public Policy at the Harvard Kennedy School, once said that “Certicom certainly can claim ownership of ECC,” noting that “[t]he algorithm was developed and patented by the company’s founders, and the patents are well written and strong.”<sup>49</sup> Certicom claimed to have had “the world’s largest intellectual property portfolio for these types of [ECC] patents.”<sup>50</sup> After acquiring Certicom, BlackBerry grew that portfolio to over 500 ECC patents.<sup>51</sup>

19. Satoshi chose Certicom’s secp256k1 curve for Bitcoin’s digital signature algorithm.<sup>52</sup> According to the Bitcoin wiki site, “secp256k1 was almost never used before Bitcoin became popular.”<sup>53</sup> As one commentator said, “If it wasn’t for Satoshi Nakamoto, you probably would never have heard of the secp256k1 Elliptic Curve Cryptography (ECC) method.”<sup>54</sup> Even

---

<sup>46</sup> <https://www.cnet.com/tech/tech-industry/certicom-creates-standards-body/>.

<sup>47</sup> See, e.g., <https://www.metzdowd.com/pipermail/cryptography/2004-April/006798.html>; <https://news.profoundimpact.com/tag/dr-scott-vanstone/>; <https://cpl.thalesgroup.com/partners/rim-certicom>.

<sup>48</sup> See <https://www.hks.harvard.edu/faculty/bruce-schneier>.

<sup>49</sup> <https://betanews.com/2007/05/30/certicom-patent-suit-against-sony-threatens-to-unravel-aacs/>.

<sup>50</sup> <https://www.certicom.com/content/certicom/en/about/news/release/2007/certicom-announces-executive-changes.html>.

<sup>51</sup> <https://blackberry.certicom.com/en>.

<sup>52</sup> See, e.g., <https://medium.com/asecuritysite-when-bob-met-alice/the-bluffers-guide-to-secp256k1-when-satoshi-said-goodbye-to-pki-bad327c4f079>; <https://news.ycombinator.com/item?id=28813291>.

<sup>53</sup> <https://en.bitcoin.it/wiki/Secp256k1>.

<sup>54</sup> <https://medium.com/asecuritysite-when-bob-met-alice/the-bluffers-guide-to-secp256k1-when-satoshi-said-goodbye-to-pki-bad327c4f079>.

Dan Brown was surprised to learn that Bitcoin uses secp256k1 instead of other, more commonly used parameters.<sup>55</sup> Some suggest that Satoshi, having not received a recommendation for a specific curve, just “picked one.”<sup>56</sup> Others suggest that Satoshi relied on expert cryptographers in selecting secp256k1.<sup>57</sup>

20. Whatever the reason, Satoshi’s choice of secp256k1 has proven to be well-liked by the Bitcoin community and the broader cryptocurrency community. The Bitcoin wiki site reports that after Bitcoin’s adoption of secp256k1, the curve “is now gaining in popularity due to its several nice properties.”<sup>58</sup> Gregory Maxwell, a former Bitcoin developer, said in a public forum in October 2021 that Satoshi’s choice of secp256k1 “was a good choice at the time, esp[ecially] now after the expiration of the GLV patent.”<sup>59</sup> “The GLV patent” refers to another groundbreaking innovation by Certicom’s in-house experts in elliptic curve cryptography, famously known as “GLV Endomorphism,”<sup>60</sup> which the Bitcoin community had been stalking for a decade or more after Hal Finney, foundational Bitcoin developer (and receiver of the first ever Bitcoin transaction), discovered in early 2011 that it can be used to speed up signature verifications by 25%.<sup>61</sup>

21. Finney, a well-known and highly respected cryptographer, posted on February 8, 2011 that he figured out a way to speed up ECDSA signature verification for the secp256k1 curve

---

<sup>55</sup> <https://bitcoinmagazine.com/technical/satoshis-genius-unexpected-ways-in-which-bitcoin-dodged-some-cryptographic-bullet-1382996984> (quoting Brown as saying “I did not know that BitCoin is using secp256k1. Indeed, I am surprised to see anybody use secp256k1 instead of secp256r1.”).

<sup>56</sup> <https://learnmeabitcoin.com/technical/cryptography/elliptic-curve/> (quoting email between Satoshi and Mike Hearn, a “Bitcoin developer” who published his emails with Satoshi).

<sup>57</sup> <https://cointelegraph.com/news/satoshi-nakamoto-had-outside-cryptography-help-says-early-bitcoin-dev> (citing Laszlo Hanyecz’s account of his conversations with Satoshi).

<sup>58</sup> <https://en.bitcoin.it/wiki/Secp256k1>.

<sup>59</sup> <https://news.ycombinator.com/item?id=28813291>.

<sup>60</sup> The Asserted Patents’ inventions are independent from and not described in the GLV patent.

<sup>61</sup> <https://btctimes.com/hal-finneys-proposal-for-optimizing-bitcoin-to-be-enabled-in-bitcoin-core/>.

used by Bitcoin, based on techniques described in “Guide to Elliptic Curve Cryptography” by Hankerson, Menezes and Vanstone.<sup>62</sup> The “Vanstone” of the book’s authoring trio is Scott Vanstone, co-founder of Certicom and co-inventor of several of the Asserted Patents in this case. The technique that Finney’s post referred to is famously known among the Bitcoin community and elsewhere as “GLV Endomorphism” or the “GLV method,” where “GLV” refers to the trio of Certicom innovators that came up with it: Robert Gallant, Robert Lambert, and Scott Vanstone.<sup>63</sup> All three were Certicom technologists and are co-inventors of several of the Asserted Patents in this case. It is widely reported that Finney’s proposed inclusion of GLV Endomorphism in the Bitcoin protocol, though it was eventually included in the Bitcoin Core software library named libsecp256k1, was not officially implemented at the time because of concerns that it would infringe “the GLV patent,” *i.e.*, U.S. Patent No. 7,110,538, which names Gallant, Lambert, and Vanstone as the inventors.<sup>64</sup> On the day the GLV patent expired, and over the days that followed, the Bitcoin community celebrated the anticipated inclusion of GLV Endomorphism in future Bitcoin Core releases.<sup>65</sup> In fact, on the day the GLV patent expired, the Bitcoin Core community began the process of deleting the “slower non-endomorphism code” and replacing it with the faster “GLV optimization,” including by deleting the code that previously made GLV endomorphism optional, thereby enabling GLV Endomorphism by default.<sup>66</sup> Others in the Bitcoin community later confirmed Finney’s observations that GLV Endomorphism results in significantly faster signature

---

<sup>62</sup> *Id.*; see also <https://cointelegraph.com/news/one-of-hal-finney-s-lost-contributions-to-bitcoin-core-to-be-resurrected>.

<sup>63</sup> See *id.*

<sup>64</sup> See *id.*

<sup>65</sup> See *id.*

<sup>66</sup> <https://github.com/bitcoin-core/secp256k1/pull/826> (“As the patent on the GLV optimization has expired, there is no need to keep the slower non-endomorphism code around anymore.”).

verifications (reportedly by 28%).<sup>67</sup> Following Bitcoin’s lead, others in the crypto community followed suit in adopting GLV Endomorphism optimizations.<sup>68</sup>

22. While some people like Finney, Malmi, and Hearn are known as early Bitcoin developers, Satoshi Nakamoto is credited with creating the first Bitcoin client, *i.e.*, the first software implementing the Bitcoin protocol.<sup>69</sup> Satoshi announced the release of the first version of Bitcoin software to the “cryptography” community on January 8, 2009.<sup>70</sup> Satoshi’s original Bitcoin software is the foundation of today’s *de facto* authoritative reference implementation of the Bitcoin protocol, known as “Bitcoin Core.”<sup>71</sup> Bitcoin Core continues to implement ECC digital signatures using ECDSA with secp256k1.<sup>72</sup>

23. The public history of Bitcoin’s development discussed above shows the impact that Certicom’s innovations had on the shaping of Bitcoin and is a testament to the bona fides of Certicom’s innovators as significant contributors to the advancement of important and valuable ECC technology.

### ***Blackberry Acquired Certicom Following Their Years-Long Alliance***

24. Blackberry was an early adopter of Certicom’s ECC technology. In July 2000, in recognition of “Certicom’s high performance, efficient ECC,” Blackberry and Certicom entered into “an alliance which will enable RIM to utilize Certicom’s elliptic curve cryptography (ECC)

---

<sup>67</sup> <https://btctimes.com/bitcoin-upgrade-glv-enomorphism-tests-show-faster-verification/>.

<sup>68</sup> See <https://github.com/RustCrypto/elliptic-curves/issues/211> (“bitcoin-core/secp256k1 is now switching to the endomorphism implementation by default: bitcoin-core/secp256k1#826 I think it would make sense for us to do the same.”).

<sup>69</sup> [https://en.bitcoin.it/wiki/Satoshi\\_Nakamoto](https://en.bitcoin.it/wiki/Satoshi_Nakamoto).

<sup>70</sup> <https://satoshi.nakamotoinstitute.org/emails/cryptography/16/>.

<sup>71</sup> [https://en.bitcoin.it/wiki/Bitcoin\\_Core](https://en.bitcoin.it/wiki/Bitcoin_Core) (Bitcoin Core is “based on the original reference code by Satoshi Nakamoto”); <https://bitcoincore.org/en/about/> (“[Bitcoin Core] is a direct descendant of the original Bitcoin software client released by Satoshi Nakamoto after he published the famous Bitcoin whitepaper.”).

<sup>72</sup> [https://en.bitcoin.it/wiki/Elliptic\\_Curve\\_Digital\\_Signature\\_Algorithm](https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm); <https://en.bitcoin.it/wiki/Secp256k1>

technology throughout its wireless product offerings.”<sup>73</sup> Blackberry recognized that “Certicom’s Elliptic Curve Cryptography (ECC) technology enables strong, high performance security for many pieces of the computing infrastructure,” and that “Certicom’s patented implementation of ECC technology provides a more efficient alternative to conventional public key cryptographic algorithms ... allowing for faster processing speed, reduced bandwidth usage and decreased battery requirements.”<sup>74</sup> Accordingly, BlackBerry entered into an “agreement with Certicom, a leader in ECC wireless security technology, [to] enable [BlackBerry] to provide the market with the secure mobile devices they require for m-commerce transactions.”<sup>75</sup>

25. In 2009, BlackBerry acquired Certicom, giving rise to BlackBerry Certicom, “a leader in applied cryptography and key management.”<sup>76</sup> Certicom’s industry-leading research and development continued under BlackBerry Certicom; together BlackBerry and Certicom continued innovating and improving ECC technology. As a result of its rich history in ECC technology development, “BlackBerry Certicom has industry leading expertise in Elliptic Curve Cryptography and has established the world’s largest ECC-based patent portfolio.”<sup>77</sup> Plaintiff Malikie now owns part of that portfolio, including the Asserted Patents.

### *Cryptocurrency Basics*

26. Bitcoin paved the way for the thousands of cryptocurrencies that exist today. The term “cryptocurrency,” or “crypto” for short, refers to a category of “digital money” that, like the fundamental purpose of Bitcoin, “makes it possible to transfer value online without the need for a

---

<sup>73</sup> <https://www.certicom.com/content/certicom/en/about/news/release/2000/research-in-motion-and-certicom-to-enable-trusted-mobile-commerc.html>.

<sup>74</sup> *Id.*

<sup>75</sup> *Id.*

<sup>76</sup> <https://www.certicom.com/content/certicom/en/about.html>.

<sup>77</sup> *Id.*; see <https://blackberry.certicom.com/en>.

middleman like a bank or payment processor.”<sup>78</sup> Most cryptocurrencies, including Bitcoin, are decentralized (not managed or controlled by a government or other central authority), not backed by anything of independent value (such as gold), and not guaranteed by anyone (such as a government or bank). Instead, cryptocurrencies are managed by “peer-to-peer networks of computers running free, open-source software.”<sup>79</sup> Specifically, cryptocurrency transactions are vetted and recorded using a technology called “blockchain,” which is a decentralized database system that stores data in a distributed network of computers. This is in some ways analogous to the ledger of accounts and transactions maintained by a traditional financial intermediary (such as a bank or credit card company). However, unlike with a traditional intermediary where the security of transactions and accounts is vested solely in the intermediary (which requires its customers to trust the intermediary with their money), the security of blockchain transactions is effected by the use of cryptography and “consensus” mechanisms to ensure that a majority of the computers on the network agree that a transaction is valid before it is recorded (*i.e.*, deemed to have occurred).<sup>80</sup>

27. As the name suggests, cryptocurrencies fundamentally rely on concepts from cryptography and computer science to enable the creation of such decentralized, internet-based monetary systems that are secure. Indeed, as stated on the Ethereum website, the world’s second most popular cryptocurrency, “[t]he reason assets such as bitcoin and ether are called ‘cryptocurrencies’ is that the security of your data and assets is guaranteed by cryptography, not by trusting an institution or corporation to act honestly.”<sup>81</sup> Cryptocurrencies rely on cryptography

---

<sup>78</sup> <https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency>.

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

<sup>81</sup> <https://ethereum.org/en/what-is-ethereum/> (answering “What is a cryptocurrency?”); *see also* <https://www.coinbase.com/learn/crypto-basics/what-is-cryptography> (“Cryptocurrencies are entirely based on cryptographic ideas.”).

(hence the name *cryptocurrency*) to protect participants' assets from theft and to protect the cryptocurrency system from dishonest or unauthorized manipulation that results in dilution of the currency (*e.g.*, double spending).<sup>82</sup> More fundamentally, cryptography is what enables cryptocurrencies like Bitcoin to be “trustless,” *i.e.*, what allows cryptocurrency to be transacted securely (even between strangers) without the need for a trusted intermediary to verify and process payments.<sup>83</sup>

### ***Transactions***

28. The role of cryptography as a fundamentally enabling technology in cryptocurrencies like Bitcoin is evident in how cryptocurrency transactions are processed, *i.e.*, initiated, validated, and recorded in the blockchain. Unlike with typical currencies, where transactions transfer an amount of currency from one account to another that is redeemable in physical notes and coins, “cryptocurrency transactions are simply data entries recorded on an unchangeable, distributed ledger, referred to as a blockchain.”<sup>84</sup> That is, with cryptocurrencies, “no cryptocurrency is actually exchanged between people. Instead, ownership data associated with both parties' crypto wallets is updated on the blockchain each time a transaction is processed.”<sup>85</sup>

29. A cryptocurrency transaction—transferring crypto from the sender's digital wallet to the receiver's digital wallet—involves several steps. Using wallet software, a transaction (essentially, a bundle of data) is created that identifies the sender's address (using a public key), the recipient's address (also using a public key), and the amount of cryptocurrency to be sent.<sup>86</sup> The transaction requestor then creates a digital signature for the transaction with its private key

---

<sup>82</sup> See <https://www.coinbase.com/learn/crypto-basics/what-is-cryptography>.

<sup>83</sup> See *id.*

<sup>84</sup> <https://www.kraken.com/learn/how-do-cryptocurrency-transactions-work>.

<sup>85</sup> *Id.*

<sup>86</sup> *Id.*



and public key (which are cryptographically linked, as the private key is used to create the public key) and submits the signed transaction to the blockchain network for validation. By signing the transaction with its private key, the requestor proves to the receiving party and to the blockchain network that the transaction is valid. After the receiving party validates the transaction using the sender's public key, the transaction is broadcast to and propagated through the blockchain network, where a majority network nodes must independently verify that the transaction is valid in order for the transaction to be added to the next "block" of the blockchain and thus be permanently and irreversibly recorded.<sup>87</sup>

### ***Wallets***

30. A cryptocurrency "wallet" is a tool for interacting with a Blockchain network that allows a user to send and receive cryptocurrencies like Bitcoin.<sup>88</sup> A wallet is typically an application (software) that functions as a wallet for storing the user's private keys and provides interfaces to access and perform transactions with the user's cryptocurrency. Wallets can be custodial (keys are managed by a third party) or non-custodial (keys are managed solely by the user). Forms of hardware wallets also exist (*e.g.*, a USB drive wallet). Crypto wallets don't store the actual cryptocurrency (because the cryptocurrency exists as data in the blockchain) but instead store the public and private keys needed to carry out crypto transactions on the blockchain.<sup>89</sup>

### ***Private Keys and Public Keys***

31. Private keys and public keys are related but different pieces of information used in cryptocurrency transactions. They are part of a technique known as asymmetric cryptography, in which two keys are used: (1) a private key (possessed by only the entity wishing to prove its

---

<sup>87</sup> *See id.*

<sup>88</sup> <https://www.investopedia.com/terms/b/bitcoin-wallet.asp>.

<sup>89</sup> *See id.*

identity) and (2) a public key (possessed by any number of entities who wishes to verify the identity of the entity possessing the private key).<sup>90</sup> Unlike the alternative approach known as symmetric cryptography—in which a single key is used by both (or all) parties for their respective purposes, thereby preventing the key from being associated with a unique identity—asymmetric cryptography simplifies key exchange by reducing the number of keys needed to secure messages between parties and allows a message signature to be uniquely authenticated (*i.e.*, associated with the unique identity of the sender).<sup>91</sup>



**SYMMETRIC**

Symmetric cryptography has an equation of  $\frac{n(n-1)}{2}$  for the number of keys needed. In a situation with 1000 users, that would mean **499,500 keys**.



**ASYMMETRIC**

Asymmetric cryptography, using key pairs for each of its users, has  $n$  as the number of key pairs needed. In a situation with 1000 users, that would mean **1000 key pairs**.

ECC Primer at 5

32. Importantly, while the public key can be used by an entity to verify that another possesses the corresponding private key, “you cannot derive the private key from the public. This is the critical feature of asymmetric cryptographic schemes that makes them so useful.” ECC Primer at 4; *see also id.* (“The critical feature of asymmetric cryptography, that makes it useful, is

<sup>90</sup> <https://www.certicom.com/content/dam/certicom/images/pdfs/WP-ECCprimer.pdf> (“ECC Primer”) at 4.

<sup>91</sup> *Id.* at 4–5.

this key pair—and more specifically, a particular feature of the key pair: the fact that one of the keys cannot be obtained from the other.”). It is also “the core technology behind digital signatures.” *Id.* “A digital signature is a transform performed on a message using the private key, whose integrity may be verified with the public key.” *Id.* at 5.



ECC Primer at 5

Elliptic curve cryptography (ECC) is an approach to doing asymmetric cryptography, including for use with digital signatures. *Id.*

33. Private and public keys form a related key-pair—a public key is generated from a private key through a one-way hash function (or “trapdoor function”) that is relatively easy to solve in one direction but nearly impossible to solve in the other direction, making it nearly impossible to determine a private key from a public key.<sup>92</sup> *See also* ECC Primer at 6-7 (“In all asymmetric cryptographic schemes, this property—the property that one key is used for encryption, and another for decryption, and the decryption key cannot be found from the encryption key—is derived from the use of mathematical functions whose inverse is extremely difficult to calculate. You may understand an asymmetric cryptographic key pair as a pair of numbers which have some relationship associated with a mathematical function which is relatively easy to compute in one direction, but whose inverse is in practical terms intractable. This feature—the function which is tractable in one direction, but intractable in the other, is common to all asymmetric cryptosystems, including ECC.”). This characteristic of asymmetric cryptography

<sup>92</sup> <https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys>.

allows the sender of cryptocurrency to digitally sign a transaction using their unique and secret private key as proof of ownership, and it allows the recipient and blockchain nodes to verify the digital signature and validate the transaction using the sender's public key. Accordingly, in cryptocurrency transactions, public keys are used to identify the sending and receiving addresses (akin to account numbers in a bank), and private keys are used to sign transactions when sending cryptocurrency to others (which can be verified by the receiver and the blockchain network using the sender's public key).<sup>93</sup>

### ***Blockchain***

34. Cryptocurrencies like Bitcoin are based on a technology called “blockchain.”<sup>94</sup> A blockchain is essentially a distributed database that, in a cryptocurrency network like Bitcoin, contains a list or “ledger” of all historical transactions on the network (*i.e.*, a record of every time anyone sent or received bitcoin). The blockchain of a cryptocurrency like Bitcoin is in some ways akin to the ledger or balance sheet of a bank.

35. A blockchain network includes a number of distributed computers (called “nodes”) that store a copy of the blockchain ledger and participate in the verification and recording of each transaction.<sup>95</sup> To become part of the blockchain ledger, a transaction must be transmitted to the network of nodes, which work to confirm the validity of the transaction using cryptographic algorithms. Valid transactions are collected into a fixed-size data file called a “block” (akin to a page of a ledger) that, once filled, is run through a cryptographic hash function (that is, the block is “hashed”) to generate a unique hash value for that block. That block's hash value is included within the next block that is created so that when the next block is hashed, its hash value depends

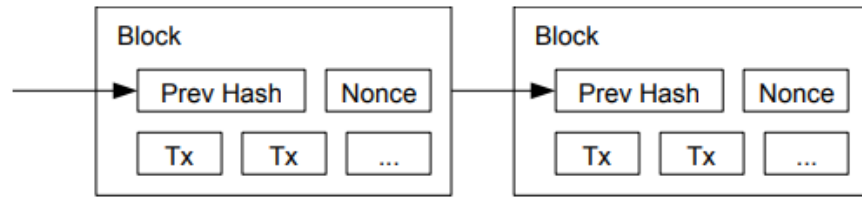
---

<sup>93</sup> *See id.*

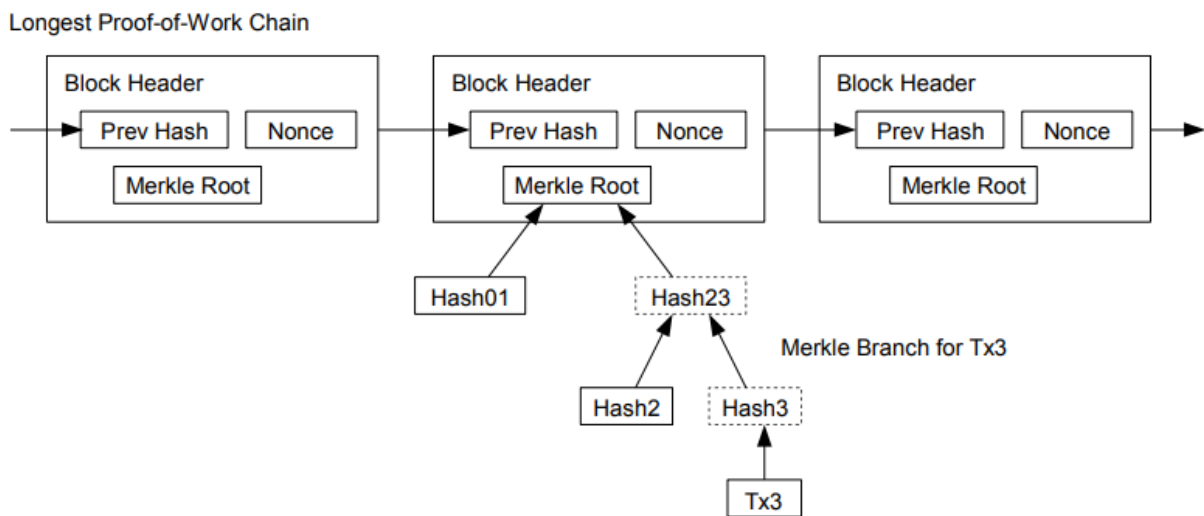
<sup>94</sup> *See* <https://www.investopedia.com/terms/b/blockchain.asp>.

<sup>95</sup> *See id.*

on the hash of the previous block, thereby creating an irreversible “chain” of blocks (hence the name “blockchain”) as the process continues.<sup>96</sup> *See also* Bitcoin Whitepaper at 2–5.



Bitcoin Whitepaper at 3



Bitcoin Whitepaper at 5

36. The Bitcoin blockchain creates a chronological ledger of chained transactions where each new block depends on the information from all previous blocks, thereby making it nearly impossible to undo or manipulate historical transactions without permission.<sup>97</sup> *See also* Bitcoin Whitepaper at 2–3 (“Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.”), *id.* (“To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it

<sup>96</sup> *See id.*

<sup>97</sup> *See id.*

and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.”).

***Bitcoin’s Consensus Mechanism: Proof of Work (“Mining”)***

37. “‘Proof of work’ and ‘proof of stake’ are the two major consensus mechanisms cryptocurrencies use to verify new transactions, add them to the blockchain, and create new tokens.”<sup>98</sup> “Proof of work, first pioneered by Bitcoin, uses mining to achieve those goals.”<sup>99</sup> In a proof of work blockchain, members of the network (“miners”) race against each other to be the first to solve a complex cryptographic math problem for determining a hash value associated with a particular block of transactions and present their solution to the network.<sup>100</sup> If the miner’s solution is verified by the network, the miner is allowed to create a new block (containing the transactions verified by the miner) and broadcast it to the network. The nodes on the network will then perform audits of the ledger and the new block, and if the auditing nodes agree, the new block is “chained” to the previous block (creating a chronological chain of transactions) and the miner is rewarded with a unit of “coin” (*i.e.*, cryptocurrency), consisting of a mining fee for solving the block, as well as transaction fees for processing the underlying transactions, as compensation for expending their resources (*e.g.*, energy) in the performance of this work. As the block chain grows, mining the next block to receive its reward becomes more computationally expensive (and therefore more resource intensive). Accordingly, the proof-of-work consensus model is more rewarding for those with more resources to deploy.<sup>101</sup>

---

<sup>98</sup> <https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake>.

<sup>99</sup> *Id.*

<sup>100</sup> *See id.*; Bitcoin Whitepaper at 3–4; <https://www.investopedia.com/terms/b/blockchain.asp>.

<sup>101</sup> *See id.*

**MARA is One of the World’s Largest Bitcoin Miners**

38. MARA is one of the largest Bitcoin miners in the world. MARA owns and/or operates multiple mining facilities in the United States that utilize more than 270,000 specialized bitcoin mining computers (“miners”) that are collectively capable of performing more than 47 exahashes per second (EH/s)—that’s 47 quintillion (47,000,000,000,000,000,000) cryptographic calculations per second.<sup>102</sup> Globally, MARA claims to operate 6.6% of the Bitcoin network with 309,334 operational miners capable of performing 53.7 EH/s.<sup>103</sup>

39. According to MARA, “[o]ur core business is bitcoin mining, and we produce, or ‘mine,’ bitcoin using one of the industry’s largest and most energy-efficient fleets of specialized computers ....” <https://ir.mara.com/sec-filings/all-sec-filings/content/0001507605-25-000003/0001507605-25-000003.pdf> (“MARA 2025 10-K”) at 6; *id.* at 33 (“We believe we are the world’s largest publicly traded bitcoin mining company, with the majority of our production in the United States.”) (“Historically, we were focused on establishing MARA as the largest and most efficient bitcoin miner.”). According to MARA, “[a]s of December 31, 2024, [MARA] operated approximately 400,000 mining rigs globally, with an energized hashrate of approximately 53.2 exahashes per second (“EH/s”)” and in 2024 “mined 9,430 bitcoin.” *Id.* at 7. MARA has located a “substantial” number of its bitcoin miners in the state of Texas because of the “generally favorable regulatory environments for bitcoin miners compared to other states.” *Id.* at 12.

40. MARA describes Bitcoin and the Bitcoin mining process as follows:

Bitcoin is a decentralized digital asset that operates on a peer-to-peer network, allowing users to send and receive payments without the need for banks and other intermediaries. Bitcoin is not linked to any fiat currency or country’s monetary policy and therefore serves as a store of value outside of government control. This is possible by

---

<sup>102</sup> <https://www.mara.com/operations#global-fleet>.

<sup>103</sup> *See id.*

using blockchain technology, which is a distributed ledger that records and verifies all transactions on the network.

The Bitcoin blockchain is a public, transparent, and unalterable record of all transactions that have ever occurred on the peer-to-peer network. When a user sends a transaction on the Bitcoin network, it is broadcast to the network and added to a pool of unconfirmed transactions known as the “mempool.” Miners, which operate specialized hardware, known as bitcoin mining rigs or application-specific integrated circuits (“ASICs”), then compete to process these unconfirmed transactions into a “block.” The first miner to successfully confirm and assemble the transactions into a block receives a reward in the form of newly minted bitcoin (block subsidy) and transaction fees. Each confirmed transaction is cryptographically signed and permanently recorded in the blockchain as a new block, and cannot be altered or deleted.

The blockchain is maintained by a robust and public open-source architecture consisting of a network of computers, known as nodes, that work together to verify and validate new transactions. Because the blockchain is decentralized and transparent, all users can verify the legitimacy of a transaction without having to rely on a third party. This eliminates the need for intermediaries, which can be slow and expensive, and makes the network resistant to censorship and fraud.

*Id.* at 6-7.

41. According to MARA, “[b]itcoin mining ... provid[es] the computational power needed to verify transactions and add new blocks to the blockchain.” *Id.* at 7. As a bitcoin mining company, MARA “provides transaction verification services to the transaction requestor, in addition to the Bitcoin network.” *Id.* at F-23. This is part of MARA’s “major” or “central” operation. *Id.* at F-3. As such, “[MARA’s] revenues are generally comprised of block rewards earned in bitcoin as a result of successfully solving blocks, and transaction fees earned for verifying transactions in support of the blockchain.” *Id.* at 35.



### **MARA's Use of the Patented Technologies**

42. On information and belief, MARA engages and has engaged in bitcoin mining activities since at least 2017 or 2018.<sup>104</sup> <sup>105</sup> On information and belief, MARA engages and has engaged in bitcoin mining using specialized mining computers, including those which it describes as its “internal mining pool,” “Company-operated mining pool,” or “MaraPool.” MARA 2025 10-K at 6, 20, F-24, F-35. On information and belief, MARA’s mining activities include and have included verifying bitcoin transactions, *id.* at 6–7, 22, 35, F-3, F-22–F-24, including verifying digital signatures consistent with the Bitcoin protocol using ECDSA and secp256k1, *see, e.g., id.* at 7, 12, 16, 19 (referring to open-source Bitcoin software and architecture).<sup>106</sup> On information and belief, at least from September 2021 until May 2022, MARA operated a mining pool that also utilized computing resources from unrelated third parties, through which MARA provided transaction verification services to transaction requestors and the Bitcoin network. MARA 2025 10-K at F23-24.

43. On information and belief, MARA generates and has generated digital signatures, including digital signatures consistent with the Bitcoin protocol using ECDSA and secp256k1, including for generating bitcoin transactions. For example, MARA sells and has sold bitcoin. *See, e.g.,* <https://ir.mara.com/sec-filings/all-sec-filings/content/0001628280-24-007680/mara-20231231.htm> (“MARA 2024 10-K”) at 26 (“[W]e are now selling periodically as a means of generating cash for our operations. By selling bitcoin outright, we can realize 100% of the then value of our

---

<sup>104</sup> *See* <https://www.mara.com/posts/from-genesis-to-global-impact-marathon-digital-evolution>; <https://www.mara.com/posts/the-road-to-23-exahash-short-film-marathon-digital-holdings>.

<sup>105</sup> MARA’s history as a bitcoin miner, as well as its history of transacting in bitcoin (buying and selling, transferring and receiving, etc.), is also described in its publicly available annual 10-K filings with the SEC from 2011–2024, which are incorporated here by reference.

<sup>106</sup> *See also, e.g.,* [https://en.bitcoin.it/wiki/Protocol\\_documentation#Transaction\\_Verification](https://en.bitcoin.it/wiki/Protocol_documentation#Transaction_Verification); [https://en.bitcoin.it/wiki/Elliptic\\_Curve\\_Digital\\_Signature\\_Algorithm](https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm); <https://en.bitcoin.it/wiki/Secp256k1>.

bitcoin when addressing liquidity needs.”), 41 (“From time to time, the Company sells bitcoin to offset its monthly cash operating costs. During the year ended December 31, 2023, the Company sold 9,482 bitcoin for total proceeds of \$264.9 million.”), 52 (“The Company ... will also continue to sell bitcoin as a means of generating cash to fund monthly operating costs and for general corporate purposes. The Company ... may buy and sell bitcoin from time to time (separately from what is outlined above) for treasury management purposes.”).

44. On information and belief, MARA uses digital asset wallets for receiving and selling bitcoin. *See, e.g.*, MARA 2025 10-K at F-3 (“We confirmed the year-end digital asset balances directly with the custodians of the Company’s wallets.”), F-12 (“The Company tracks its cost basis of digital assets by-wallet in accordance with the first-in-first-out method of accounting.”), F-12–F-24 (“The MaraPool wallet (owned by the Company as Operator) is recorded on the distributed ledger as the winner of proof of work block rewards and assignee of all validations and, therefore, the transaction verifier of record.”); *see id.* at 22 (“Digital assets are controllable only by the possessor of both the unique public key and private key relating to the local or online digital wallet which hold the digital assets.”); MARA 2024 10-K at F-19 (“On June 10, 2022, the Company redeemed 100% of its limited partnership interest in the Fund in exchange for approximately 4,769 bitcoin with a fair market value of approximately \$137.8 million. This bitcoin was transferred from the Fund’s custodial wallet to the Company’s digital wallet.”). On information and belief, MARA regularly transfers digital assets to or from other entities, including vendors, consultants and services providers. MARA 2025 10-K at 23.

45. MARA began engaging in the foregoing infringing activities years after Certicom and BlackBerry invented and received patents covering the ECC technologies at issue in this

action. Indeed, most of these innovations were already incorporated into the Bitcoin protocol and architecture by the time MARA began its Bitcoin mining operations.

46. On information and belief, the accused activities are important parts of MARA's core business, its "major" or "central" operations, and its general source of revenue. MARA 2025 10-K at 35, F-3.

### **PATENTS IN SUIT**

47. Malikie is the assignee of and owns all right and title to U.S. Patent Nos. 8,788,827 (the "'827 Patent"); 10,284,370 (the "'370 Patent"); 7,372,960 (the "'960 Patent"); 8,666,062 (the "'062 Patent"); 7,372,961 (the "'961 Patent"); and 8,532,286 (the "'286 Patent") (collectively, the "Asserted Patents").

48. The Asserted Patents, now owned by Malikie, were originally assigned to Certicom. Their inventors are former Certicom employees who spearheaded Certicom's industry-leading research and development in elliptic curve cryptography, applied cryptography and key management, and other data security technologies. After a longstanding alliance between BlackBerry and Certicom that enabled BlackBerry to utilize Certicom's elliptic curve cryptography technology in its products, BlackBerry acquired Certicom in 2009.<sup>107</sup> Through its acquisition of Certicom and continued research and development in ECC, key management, and other aspects of data security, BlackBerry amassed "the world's largest ECC-based patent portfolio,"<sup>108</sup> which grew to include over 500 ECC patents<sup>109</sup>.

---

<sup>107</sup> See <https://www.certicom.com/content/certicom/en/about.html>; <https://www.certicom.com/content/certicom/en/about/news/release/2000/research-in-motion-and-certicom-to-enable-trusted-mobile-commerce.html>.

<sup>108</sup> <https://www.certicom.com/content/certicom/en/about.html>.

<sup>109</sup> <https://blackberry.certicom.com/en>.

49. Certicom and BlackBerry developed numerous innovative and diverse technologies, including groundbreaking inventions pertaining to generating and verifying digital signatures and related cryptographic and data security technology. Some of these groundbreaking inventions are described and claimed in certain of the Asserted Patents.

**The “Accelerated Verification Patents” (’827, ’370)**

50. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

51. The ’827 Patent, entitled “Accelerated Verification of Digital Signatures and Public Keys,” was duly and lawfully issued on July 22, 2014. A true and correct copy of the ’827 Patent is attached hereto as Exhibit 1. The application for the ’827 Patent was filed on September 14, 2012 and claims the benefit of priority to earlier related applications, including provisional application no. 60/644,034, filed on January 18, 2005.

52. The ’827 Patent has been and continues to be in full force and effect since its issuance. Malikie owns by assignment the entire right and title in and to the ’827 Patent, including the right to seek damages for any infringement thereof.

53. The ’370 Patent, entitled “Accelerated Verification of Digital Signatures and Public Keys,” was duly and lawfully issued on May 7, 2019. A true and correct copy of the ’370 Patent is attached hereto as Exhibit 2. The application for the ’370 Patent was filed on June 27, 2014 as a continuation of the ’827 Patent.

54. The ’370 Patent has been and continues to be in full force and effect since its issuance. Malikie owns by assignment the entire right and title in and to the ’370 Patent, including the right to seek damages for any infringement thereof.

55. The '827 Patent and '370 Patent (the “Accelerated Verification Patents”) share the same title, specification, inventors, and a common priority claim.

56. The Accelerated Verification Patents relate to computational techniques used in cryptographic algorithms, including elliptic curve algorithms for generating and verifying digital signatures, that enable accelerated digital signature verification. *See, e.g.*, Ex. 1 at 1:12-13, 4:15-33, 9:32-37, 11:43-50, 12:47-59, 13:60-62, 14:40-42, 15:27-40.<sup>110</sup>

57. Cryptographic algorithms for generating and verifying digital signatures are used in cryptographic systems (or “cryptosystems”) to secure electronic data in computer systems and computer networks. *See, e.g.*, Ex. 1 at 1:18-48; *see also, e.g.*, 2:17-3:17, 6:23-36. The nature of electronic data in computer systems and computer networks presents unique security concerns relating to, for example, digital message authenticity, for which specialized digital signature techniques were found to be necessary. *See, e.g.*, Ex. 1 at 1:18-48; *see also, e.g., id.* at 2:17-3:17; Whitfield Diffie and Martin Hellman, *New Directions in Cryptography* (1976)<sup>111</sup> at 645 (“Current electronic authentication techniques cannot meet this need.”), 647 (“Unforgeable digital signatures and receipts are needed.”), 649 (“Current electronic authentication systems cannot meet the need for a purely digital, unforgeable, message dependent signature. They provide protection against third party forgeries, but do not protect against disputes between transmitter and receiver.”), 649 (observing that “we must discover a digital phenomenon” to provide authentication for a “purely electronic form of communication”).

---

<sup>110</sup> Citations to the Accelerated Verification Patents (Exhibits 1 and 2) are exemplary and non-limiting. Because the '827 Patent and '370 Patent share a common specification, only the '827 Patent (Exhibit 1) is cited in this Section. Citations to Exhibit 1 in this Section are intended to be representative of the Accelerated Verification Patents.

<sup>111</sup> <https://ee.stanford.edu/~hellman/publications/24.pdf> (“*New Directions in Cryptography*”).

58. Digital signatures are generated using public key cryptography, *see, e.g.*, Ex. 1 at 1:18-48; *see also, e.g., id.* at 2:17-3:17, which is a type of technology for securing electronic communications that was discovered after the advent of digital computing to address cryptography problems arising particularly in “computer controlled communication networks” that created “a need for new types of cryptographic systems.”<sup>112</sup> *New Directions in Cryptography* at 644; *see also id.* (“Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.”); <https://www.invent.org/inductees/whitfield-diffie> (“In 1976, Whitfield Diffie, Martin Hellman, and Ralph Merkle developed public key cryptography (PKC), an innovative new method for securing electronic communications.”); <https://archive.nytimes.com/www.nytimes.com/library/cyber/week/122497encrypt.html> (“The set of algorithms, equations and arcane mathematics that make up public key cryptography are a crucial technology for preserving computer privacy in and making commerce possible on the Internet. Some hail its discovery as one of the most important accomplishments of 20th-century mathematics .... Without it, there would be no privacy in cyberspace.”); Whitfield Diffie, *The First Ten Years of Public Key Cryptography* (1988)<sup>113</sup> at 560 (“Public key cryptography was born in May 1975, the child of two problems,” where “[t]he second problem ... was the problem of signatures. Could a method be devised that would provide the recipient of a purely digital electronic message with a way of demonstrating to other people that it had come from a particular person...?”); *id.* at 560 (“This

---

<sup>112</sup> Some credit Whitfield Diffie, Martin Hellman, and Ralph Merkle with discovering public key cryptography, while others credit James Ellis, Clifford Cocks, and Malcom Williamson. Diffie, Hellman, and Merkle have received multiple patents for public key cryptography techniques, including U.S. Patent Nos. 4,200,770 and 4,218,582. Other public key cryptography techniques, like RSA, have also been patented. *See, e.g.*, U.S. Patent No. 4,405,829.

<sup>113</sup> <https://www.cs.virginia.edu/~evans/greatworks/diffie.pdf> (“*The First Ten Years of Public Key Cryptography*”).

separation [of the capacities for encryption and decryption using public key cryptography] allows important improvements in the management of cryptographic keys and makes it possible to ‘sign’ a purely digital message.”); <https://bitcoinwiki.org/wiki/public-key-cryptography> (“Public key algorithms are fundamental security ingredients in modern [ ] applications and protocols assuring the confidentiality[ and] authenticity [ ] of electronic communications and data storage. They underpin various Internet standards ....”); <https://www.nsa.gov/History/Cryptologic-History/Historical/Historical-Figures-View/Article/3006218/clifford-cocks-james-ellis-and-malcolm-williamson/> (“The security of the global communication infrastructure is built on public key cryptography and the importance of PKC in enabling the modern world of secure banking, e-commerce, and encrypted messaging cannot be overstated.”).

59. As the patents explain, “Public key cryptography permits the secure communication over a data communication system without the necessity to transfer identical keys to other parties in the information exchange through independent mechanisms, such as a courier or the like.” *See, e.g.*, Ex. 1 at 1:24-34. “Public key cryptography is based upon the generation of a key pair, one of which is private and the other public that are related by a one way mathematical function.” *Id.* “The one way function is such that, in the underlying mathematical structure, the public key is readily computed from the private key but the private key cannot feasibly be ascertained from the public key.” *Id.* “Public key cryptography may also be used to digitally sign a message to authenticate the origin of the message.” *Id.* at 1:44-48. “The author of the message signs the message using his private key and the authenticity of the message may then be verified using the corresponding public key.” *Id.* So, in a network where members do not know each other (or wish to remain pseudonymous) and have never even communicated with each other previously, “[a] subscriber can sign a message by encrypting it with his own secret key. Anyone with access

to the public key can verify that it must have been encrypted with the corresponding secret key, but this is of no help to him in creating (forging) a message with this property.” *The First Ten Years of Public Key Cryptography* at 561. “The availability of a signature that the receiver of a message cannot forge and the sender cannot readily disavow makes it possible to trust the network with negotiations and transactions of much higher value than would otherwise be possible.” *Id.* Accordingly, digital signature technology based on public key cryptography fundamentally enables “trustless” networks that do not require a trusted intermediary to verify or authenticate messages.

60. The patents further explain that “[t]he security of such systems [employing digital signatures using public key cryptography] is dependent to a large part on the underlying mathematical structure.” *See, e.g.*, Ex. 1 at 1:49-55. “The most commonly used structure for implementing discrete logarithm systems is a cyclic subgroup of a multiplicative group of a finite field in which the group operation is multiplication or cyclic subgroups of elliptic curve groups in which the group operation is addition.” *Id.*

61. “An elliptic curve  $E$  is a set of points of the form  $(x,y)$  where  $x$  and  $y$  are in a field  $F$ , such as the integers modulo a prime [number]  $p$ , commonly referred to as  $F_p$ , and  $x$  and  $y$  satisfy a non-singular cubic equation, which can take the form  $y^2=x^3+ax+b$  for some  $a$  and  $b$  in  $F$ .” *Id.* at 1:56-2:16. Elliptic curves have other defining characteristics that give them special properties making them useful for cryptographic implementations. *See id.*

62. “In an elliptic curve cryptosystem,” “[t]he key pair may be used with various cryptographic algorithms to establish common keys for encryption and to perform digital signatures.” *Id.* at 2:17-27. “One such algorithm is the Elliptic Curve Digital Signature Algorithm (ECDSA) used to generate digital signatures on messages exchanged between entities. Entities



using ECDSA have two roles, that of a signer and that of a verifier.” *Id.* at 2:28-31. In ECDSA cryptosystems, “[the] signer selects a long term private key  $d$ , which ... must be secret.” *Id.* at 2:31-41. The signer also computes “ $Q$ ”, which is “the long term public key of the signer, and is made available to the verifiers.” *Id.* “Finding the private key  $d$  from the public key  $Q$  is believed to [be] an intractable problem for the choices of elliptic curves used today.” *Id.* Accordingly, “[f]or any message  $M$ , the signer can create a signature, which is a pair of integers  $(r, s)$  in the case ECDSA,” and “[a]ny verifier can take the message  $M$ , the public key  $Q$ , and the signature  $(r, s)$ , and verify whether it was created by the corresponding signer.” *Id.* at 2:42-48. This is because creation of a valid signature  $(r, s)$  is believed to possible only by an entity who knows the private key  $d$  corresponding to the public key  $Q$ .” *Id.*

63. The process for creating a digital signature (signing an electronic message) using ECDSA includes, among others, the following steps. “First, the signer chooses some integer  $k$  ... that is to be used as a session, or ephemeral, private key. The value  $k$  must be secret.” *Id.* at 2:49-63. “Then, the signer computes a point  $R=kG$  that has coordinates  $(x, y)$ .” *Id.* “Next, the signer converts  $x$  to an integer  $x'$  and then computes  $r=x' \bmod n$ , which is the first coordinate of the signature.” *Id.* “The signer must also compute the integer  $e=h(M) \bmod n$ , where  $h$  is [a] hash function.” *Id.* “Finally, the second coordinate  $s$  is computed as  $s=(e+dr)/s \bmod n$ .” *Id.* “The components  $(r, s)$  are used by the signer as the signature of the message,  $M$ , and sent with the message to the intended recipient.” *Id.*

64. The process for verifying a digital signature created using ECDSA includes, among others, the following steps. “First the verifier computes an integer  $e=h(M) \bmod n$  from the received message.” Ex. 1 at 2:64-3:4. “Then the verifier computes integers  $u$  and  $v$  such that  $u=e/s \bmod n$  and  $v=r/s \bmod n$ .” *Id.* “Next, the verifier computes a value corresponding to the point  $R$  that is

obtained by adding  $uG+vQ$ . This has co-ordinates  $(x, y)$ .” *Id.* “Finally the verifier converts the field element  $x$  to an integer  $x'$  and checks that  $r=x' \bmod n$ . If it does the signature is verified.” *Id.*

65. The inventors recognized technological problems associated with the above-described ECDSA signature verification process and invented ways to improve it. For example, the inventors recognized that “the verification of an ECDSA signature appears to take twice as long as the creation of an ECDSA signature, because the verification process involves two scalar multiplications, namely  $uG$  and  $vQ$ , whereas signing involves only one scalar multiplication, namely  $kG$ .” Ex. 1 at 3:5–17. The inventors further recognized that “[e]lliptic curve scalar multiplications consume most of the time of these processes, so twice as many of them essentially doubles the computation time.” *Id.* And, while some “[m]ethods are known for computing  $uG+vQ$  that takes less time than computing  $uG$  and  $v[Q]$  separately,” the inventors recognized that such methods nevertheless “mean that computing  $uG+vQ$  can take 1.5 times as long as computing  $kG$ .” *Id.*

66. Accelerating elliptic curve computations (reducing computing time) is a technological problem for which the inventors discovered technological solutions. Accelerating elliptic curve computations requires the use of additional computer resources, such as memory and processing capabilities. *See* Ex. 1 at 3:18-4:14. However, known techniques for accelerating elliptic curve computations provided limited overall benefits to the overall computer architecture because the ability to achieve faster operations came at the significant cost of more memory and potentially wasteful pre-computation processing cycles. *Id.* The inventors recognized that “these costs may accumulate to the point that any benefit of faster computation is offset by the need to store or communicate” more pre-computed data. Moreover, “[t]he net benefit depends on the relative cost of time, memory and bandwidth, which can vary tremendously between

implementations and systems.” *Id.* Accordingly, achieving such benefits required case-by-case optimizations of parameters to strike a balance between an achievable increase in speed with increases in computational and memory costs. *See id.*

67. The inventors taught improvements to the ECDSA digital signature verification process. Ex. 1 at 4:15-33. For example, the patents teach techniques that enable accelerated signature verification, which include, among other things, generating, for use with a digital signature (*e.g.*, a signature with components ( $r, s$ )), an indicator (*e.g.*,  $i$ ) to identify which value of a plurality of values (*e.g.*, for a point with coordinates ( $x, y$ )) recoverable from the first signature component (*e.g.*,  $r$  of the pair ( $r, s$ )) is an ephemeral public key (*e.g.*,  $R$ ). *See, e.g.*, Ex. 1 at 5:23-31, 6:37-7:38, 9:44-46, 10:61-11:5, 12:11-59, 15:29-33. The patents teach that such techniques accelerate the recovery of, for example, an ephemeral public key (*e.g.*,  $R$ ) for verifying digital signatures (thereby also accelerating digital signature verification), which provide a technological improvement. *See, e.g., id.*

68. The patents also teach techniques that enable accelerated signature verification, which include, among other things, recovering (or generating) a signer’s public key (*e.g.*,  $Q$ ) where doing so includes computing  $Q=r^{-1}(sR-eG)$ , where  $G$  comprises a generator of an elliptic curve group that includes a first elliptic curve point  $R$  and the second elliptic curve point  $Q$ . *See, e.g.*, Ex. 1 at 4:48-5:4; 7:39-58, 8:12-9:31, 9:67-10:34, 12:43-59, 13:1-26, 15:15-40. The patents teach that such techniques accelerate the verification of digital signatures, allowing more digital signatures to be verified in a given amount of time, which provide a technological improvement over preexisting techniques. *See, e.g., id.*

**The “Finite Field Engine Patents” (’960 and ’062)**

69. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

70. The ’960 Patent, entitled “Method and Apparatus for Performing Finite Field Calculations,” was duly and lawfully issued on May 13, 2008. A true and correct copy of the ’960 Patent is attached hereto as Exhibit 3. The application for the ’960 Patent was filed on January 29, 2002 and claims the benefit of priority to earlier related applications, including provisional application nos. 60/343,220, 60/343,223, and 60/343,226, and 60/343,227, all filed on December 31, 2001.

71. The ’960 Patent was in full force and effect since its issuance. Malikie owns by assignment the entire right and title in and to the ’960 Patent, including the right to seek damages for any infringement thereof.

72. The ’062 Patent, entitled “Method and Apparatus for Performing Finite Field Calculations,” was duly and lawfully issued on March 4, 2014. A true and correct copy of the ’062 Patent is attached hereto as Exhibit 4. The application for the ’062 Patent was filed on April 11, 2008 as a continuation of the ’960 Patent.

73. The ’062 Patent was in full force and effect since its issuance. Malikie owns by assignment the entire right and title in and to the ’062 Patent, including the right to seek damages for any infringement thereof.

74. The ’960 Patent and ’062 Patent (the “Finite Field Engine Patents”) share the same title, specification, inventor, and common priority claim.

75. The Finite Field Engine Patents relate generally to finite field engines and methods for use with cryptographic systems. *See, e.g.*, Ex. 3 at 1:10–13.<sup>114</sup>

76. The patents teach that “[c]ryptography is commonly used to provide data security, integrity, and authentication” over communication channels, such as, for example, connections over the Internet or a wireless network. *See, e.g., id.* at 1:16–39. Protocols employing such cryptographic technology may require the use of secret keys. *Id.* For example, “[c]orrespondents using public key cryptography each have a private key and a corresponding public key” such that “it is computationally infeasible to compute the private key given only the public key,” while “a mathematical relationship between the keys allows them to be used to provide security, integrity, or authentication in various protocols where the public keys are shared and the private keys are kept secret.” *Id.*

77. The patents teach that “[e]lliptic curve cryptography (ECC) is a particularly efficient form of public key cryptography that is especially useful in [resource] constrained environments.” *See, e.g., id.* at 1:40–55.

78. As the patents explain, an elliptic curve is specified with “a finite field and an equation over that finite field are needed,” where “[t]he points on the elliptic curve are the pairs of finite field elements satisfying the equation of the curve.” *See, e.g., id.* at 1:40–55. “To carry out calculations involving points on the elliptic curve, calculations are done in the underlying finite field, according to well-known formulas that use parameters of the curve.” *Id.* “These formulas

---

<sup>114</sup> Citations to the Finite Field Engine Patents (Exhibits 3 and 4) are exemplary and non-limiting. Because the ’960 Patent and ’062 Patent share a common specification, only the ’960 Patent (Exhibit 3) is cited in this Section. Citations to Exhibit 3 in this Section are intended to be representative of the Finite Field Engine Patents.

define an addition operation on a pair of elliptic curve points,” and “[a] scalar multiplication operation is defined by repeated additions, analogously to regular integer multiplication.” *Id.*

79. Users of an elliptic curve cryptosystem generate a key pair comprising a private key and a public key based on parameters common to all uses (including the finite field, the elliptic curve, and a generator point on the curve). *Id.* at 1:56–65. A correspondent’s private key is an integer (which is kept secret, such as a random number) that is less than the order of the elliptic curve. *Id.* “A correspondent’s public key is the elliptic curve point obtained by scalar multiplication of the private key with a generator point.” *Id.*

80. The patents teach that “[t]he security level of a cryptographic system mainly depends on the key size that is used,” where “[l]arger key sizes give a higher security level than do smaller key sizes.” *See, e.g., id.* at 1:66–2:7. “[H]owever, different key sizes require defining different elliptic curves over different finite fields,” where (generally) “the greater the desired cryptographic strength of the ECC, the larger will be the size of the finite field.” *Id.* Multiple technological problems emerge from these possibilities.

81. For example, given the possible variability in elliptic curves and finite fields, “an implementation of elliptic curve cryptography may need to support several different finite fields for use in particular applications.” *Id.* at 2:8–24. The patents teach that “[i]mplementing [such] an elliptic curve cryptosystem therefore requires either the implementation of specific methods for each finite field or a generic method usable in any finite field.” *See, e.g., id.* The patents further teach that “[t]he use of specific methods for each finite field leads to more efficient code since it may be optimized to take advantage of the specific finite field,” but that “supporting several finite fields in this way will increase the code size dramatically.” *See, e.g., id.* On the other hand, “[t]he use of a generic method prevents the use of optimization techniques, since the code cannot take

advantage of any particular properties of the finite field,” which “makes the code less efficient but has the advantage of much smaller code size.” *Id.*

82. Another technological problem is that “[s]oftware implementation of finite fields raises the question of how to arrange the storage of the bits corresponding to the finite field elements.” *Id.* at 2:25–30. The patents teach that elliptic curve cryptosystems may employ finite fields (whether binary fields or prime fields) with elements that may be represented as bits in hardware or software, where “[t]hese bits must then be represented in the memory storage of the computer system.” *See, e.g., id.* The patents teach, however, that “[w]hen using a general purpose computational engine (for example a typical CPU), finite field elements are often too long to be represented in a single machine word of the engine (engine word lengths are typically 16, 32, or 64 bit).” *See, e.g., id.* And, “[s]ince the finite field [elements] used in ECC operations are typically 160 bits or more, these elements must be represented in several machine words.” *Id.* “Engine routines (programs) that provide finite field calculations must therefore deal with multiple machine words to complete their calculations.” *Id.* Moreover, “[w]ith either type of codes,” *i.e.*, software employing specific methods (which may be word size-specific) or general methods (which may be word size non-specific), “it is necessary to provide finite field operations including multiplication, addition, inversion, squaring and modular reduction.” *Id.* To compute the results of such operations on ECC finite field elements and store them in computer memory, complicated operations and “many bit shifts are required,” which “results in longer processing time and also extra processor operation.” *Id.*

83. The inventors recognized that improvements in finite field operations, including for ECC operations, may be achievable to improve the speed and efficiency of finite field engines. Ex. 3 at 4:10–27; *see id.* at 1:66–3:30.

84. For example, the patents teach techniques that enable the performance of finite field operations (*e.g.*, addition, subtraction, multiplication) on elements of a finite field (*e.g.*, coordinates of points on an elliptic curve) that include, among other things, representing each finite field element as a predetermined number of machine words, performing a non-reducing wordsized finite field operation on the representations and completing the operation for each word to obtain an unreduced result, performing a specific modular reduction of the unreduced result to reduce it to that of a field element, and using the reduced result in a cryptographic operation. *See, e.g., id.* at 6:30–7:18, 7:19–9:7, 9:8–12:12, 15:13–16:42. Using such techniques, technological benefits are achievable. For example, “fast engines can be produced for many specific finite fields, without duplicating the bulk of the engine instructions (program).” *Id.*, Abstract, 4:22–27; *see also, e.g., id.* at 12:155–13:15, 15:12–21. Additionally, “finite field elements may be consistently stored in registers of the same word length.” *Id.* at 8:46–60. Furthermore, fewer bit shifts are required, thereby resulting in shorter processing time and fewer processor operations. *Id.* at 11:14–19, 11:34–40; *see id.* at 3:26–30.

85. The patents also teach techniques that enable the performance of finite field operations (*e.g.*, addition, subtraction, multiplication) on elements of a finite field (*e.g.*, coordinates of points on an elliptic curve) that include, among other things, obtaining a first set of instructions for performing the finite field operation on values representing the elements of the finite field and executing it to generate an unreduced result, obtaining a second set of instructions for performing a modular reduction for a specific finite field and executing it to generate a reduced result, and providing the reduced result as an output for use in a cryptographic operation. *See, e.g., id.* at 6:30–7:18, 7:19–9:7, 9:8–12:12, 15:13–16:42. Using such techniques, technological benefits are achievable. For example, “fast engines can be produced for many specific finite fields, without



duplicating the bulk of the engine instructions (program).” *Id.*, Abstract, 4:22–27; *see also, e.g., id.* at 12:155–13:15, 15:12–21. Additionally, “finite field elements may be consistently stored in registers of the same word length.” *Id.* at 8:46–60. Furthermore, fewer bit shifts are required, thereby resulting in shorter processing time and fewer processor operations. *Id.* at 11:14–19, 11:34–40; *see id.* at 3:26–30.

### **The “Ephemeral Key Generation” Patent (’961)**

86. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

87. The ’961 Patent, entitled “Method of Public Key Generation,” was duly and lawfully issued on May 13, 2008. A true and correct copy of the ’961 Patent is attached hereto as Exhibit 5. The application for the ’961 Patent was filed on December 26, 2001.

88. The ’961 Patent was in full force and effect since its issuance. Malikie owns by assignment the entire right and title in and to the ’961 Patent, including the right to seek damages for any infringement thereof.

89. The Ephemeral Key Generation Patent (the ’961 Patent) relates generally to key generation within public key cryptosystems. *See, e.g., Ex. 5* at 1:5–6.

90. The patent teaches that “[t]he basic structure of a public key cryptosystem is well known and has become ubiquitous with security in data communication systems.” *Id.* at 1:10–16. Public key cryptosystems “use a private key  $k$  and a corresponding public key  $\alpha^k$  where  $\alpha$  is a generator of the group.” *Id.*

91. A public key cryptosystem architecture can enable multiple security operations for use with electronic data in digital systems and networks to be performed, including encryption, key agreement, and authentication (e.g., digital signatures). *Id.* at 1:10–32. For example, a public

key cryptosystem architecture enables “one party [to] encrypt a message  $m$  with the intended recipients public key and the recipient may apply his private key to decrypt it.” *Id.* Such “cryptosystems may [also] be used for key agreement protocols where each party exponentiates the other party’s public key with their own private key.” *Id.* For example, “party A will take B’s public key  $\alpha^b$  and exponentiate it with A’s private key  $a$  to obtain a session key  $\alpha^{ab}$ ,” and “B will take A’s public key  $\alpha^a$  and exponentiate it with B’s private key  $b$  to obtain the same session key  $\alpha^{ab}$ ,” after which “data may be transferred using a symmetric key protocol utilizing the common session key.” *Id.* “Public key cryptosystems may also be used to sign messages to authenticate the author and/or the contents,” for example, by enabling “the sender [to] sign a message using his private key and a recipient [to] verify the message by applying the public key of the sender,” such that “[i]f the received message and the recovered message correspond then the authenticity is verified.” *Id.*

92. The patent teaches that the strength of security of public key cryptosystems is based on “the intractability of the discrete log problem in finite field arithmetic.” *Id.* at 1:33–38. In other words, “even when the generator  $\alpha$  and public key is known, it is computationally infeasible to obtain the corresponding private key,” which means that “[t]he security of such systems does therefore depend on the private key remaining secret.” *Id.*

93. “To mitigate the opportunity of disclosing the private key,” the patent teaches that “protocols have been developed that use a pair of private keys and corresponding public keys, referred to as long term and short term or ephemeral key pairs respectively.” *Id.* at 1:38–51. In such an architecture, “[t]he ephemeral private key is generated at the start of each session between a pair of correspondents, usually by a random number generator. The corresponding, ephemeral public key is generated and the resultant key pair used in one of the possible operations described

above,” such as encryption, key management, or authentication. *Id.* “The long-term public key is utilized to authenticate the correspondent through an appropriate protocol,” but “[o]nce the session is terminated, the ephemeral key is securely discarded and a new ephemeral key generated for a new session.” *Id.*

94. Protocols for using digital signatures that enable the use of long term and short term (or ephemeral) key pairs include the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). *Id.* at 1:52–2:32. However, the inventors recognized that the generation of ephemeral keys “may be done in such a way as to inadvertently introduce a bias in to the selection of [ephemeral keys]  $k$ ,” which “may be exploited to extract a value of the private key  $d$  and thereafter render the security of the system vulnerable.” *Id.* at 2:32–61. For example, the National Institute of Standards and Technology (NIST) FIPS 186-2 Digital Signature Standard (DSS) “stipulates the manner in which an integer is to be selected for use as a private key,” whereby “[a] seed value,  $SV$ , is generated from a random number generator which is then hashed by a SHA-1 hash function to yield a bit string of predetermined length, typically 160 bits.” *Id.* “The bit string represents an integer between 0 and  $2^{160}-1$ ,” where “this integer could be greater than the prime  $q$  and so the DSS requires the reduction of the integer mod  $q$ , i.e.  $k = \text{SHA-1}(\text{seed}) \bmod q$ ,” which can be expressed as: *if*  $\text{SHA-1}(\text{seed}) \geq q$  *then*  $k \leftarrow \text{SHA-1}(\text{seed}) - q$  *else*  $k \leftarrow \text{SHA-1}(\text{seed})$ . *Id.* The patent teaches that “[w]ith this algorithm it is to be expected that more values will lie in the first interval than the second and therefore there is a potential bias in the selection of  $k$ .” *Id.*

95. Problematically, this creates a security weakness based on the technological capabilities available to attackers, for example, by making it possible to guess the private key by employing enough computer resources by testing a large amount of possible ephemeral keys (*e.g.*, a brute force attack). The patent teaches that “the modular reduction to obtain [ephemeral keys]  $k$

introduces sufficient bias in to the selection of  $k$  [such] that an examination of  $2^{22}$  signatures could yield the private key  $d$  in  $2^{64}$  steps using  $2^{40}$  memory units.” *Id.*

96. The inventors recognized these technological problems and discovered improvements in ephemeral key generation technology to address them. *See* Ex. 5 at 2:60–3:3; *see generally id.* at 3:23–5:30.

97. For example, the patent teaches techniques for generating a key  $k$  for use in a cryptographic function performed over a group of order  $q$  that include, for example, generating a seed value  $SV$  from a random number generator, performing a hash function  $H()$  on the seed value  $SV$  to provide an output  $H(SV)$ , determining whether the output  $H(SV)$  is less than the order  $q$  prior to reducing mod  $q$ , accepting the output  $H(SV)$  for use as the key  $k$  if the value of the output  $H(SV)$  is less than the order  $q$ , rejecting the output  $H(SV)$  as the key if the value is not less than the order  $q$ , repeating the preceding steps if the output  $H(SV)$  is rejected, and providing the key  $k$  for use in performing the cryptographic function if the output  $H(SV)$  is accepted, wherein the key  $k$  is equal to the output  $H(SV)$ . *See, e.g.,* 3:23–4:17; *see also* 4:18–5:30. The patent teaches that such inventions provide key generation techniques in which any bias is eliminated during the selection of the key, *id.* at 3:1–3, which may, for example, be stored in secure memory and retrieved from the secure memory for use in a cryptographic protocol, such as ECDSA, for performing signatures, key exchange, or key transport operations in a public key cryptography architecture, *id.* at 3:23–63.

#### **The “Improved Modular Reduction” Patent (’286)**

98. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

99. The '286 Patent, entitled "System and Method for Reducing the Computation and Storage Requirements for a Montgomery-Style Reduction," was duly and lawfully issued on September 10, 2013. A true and correct copy of the '286 Patent is attached hereto as Exhibit 6. The application for the '286 Patent was filed on July 19, 2010, and claims the benefit of priority of Provisional App. No. 61/226,427, filed on July 17, 2009.

100. The '286 Patent has been and continues to be in full force and effect since its issuance. Malikie owns by assignment the entire right and title in and to the '268 Patent, including the right to seek damages for any infringement thereof.

101. The Improved Modular Reduction Patent (the '286 Patent) relates generally to systems and methods for reducing the computation and storage requirements for a Montgomery style reduction (a form of modular arithmetic). *See, e.g.*, Ex. 6 at 1:13–16; *see also id.*, Abstract.

102. The patent teaches that "[i]n cryptography, e.g. public key cryptography, operations such as multiplication or exponentiation of integers in some group  $Z_n$ , may be required, where modular arithmetic is used to operate on the integers." Ex. 6 at 1:20–30. "For example, to multiply two numbers modulo some [number]  $n$ , the classical approach is to first perform the multiplication and then calculate the remainder."<sup>115</sup> *Id.* The patent teaches that "[a]lthough the classical approach is simple for basic operations such as in multi-precision calculations and does not require precomputation, the step of calculating the remainder is considered slow." *Id.* "The calculation of the remainder is referred to as reduction in modular arithmetic." *Id.*

---

<sup>115</sup> The term "modulo" means to calculate the remainder after dividing one number by another. *See, e.g.*, <https://www.mathsisfun.com/definitions/modulo-operation.html>; *see also* <https://en.wikipedia.org/wiki/Modulo> ("In computing and mathematics, the modulo operation returns the remainder or signed remainder of a division, after one number is divided by another, the latter being called the modulus of the operation.")

103. The patent further teaches that “[i]n Montgomery reduction, calculations with respect to a modulus  $n$  are carried out with the aid of an auxiliary number  $R$  called the Montgomery radix or base.” Ex. 6 at 1:47–64. For example, “[t]he Montgomery reduction of a number  $a$  with radix  $R$  and prime modulus  $n$  is the quantity given by  $aR^{-1} \bmod n$ .” *Id.*

104. “In a given cryptographic system,” the patent teaches, “a computational engine may be used for calculating the Montgomery product of two numbers, this engine being sometimes referred to as a Montgomery engine or Montgomery machine.” Ex. 6 at 1:65–2:13. The patent further teaches that “[t]he engine may be implemented in a hardware or software module and operates on a set of parameters to produce a result.” *Id.* For example, using a Montgomery engine, “Montgomery multiplication may proceed as follows:

1.  $c \leftarrow 0$ , where  $c$  will hold the result  $abR^{-1} \bmod n$  and  $c = (c_k c_{k-1} \dots c_1 c_0)$ .
2. For  $i$  from 0 to  $(k-1)$  do the following:
  - 2.1  $m \leftarrow (c_0 + a_i, b_0)\mu \bmod 2^w$ ; and
  - 2.2  $c \leftarrow (c + a_i b + mn)/2^w$
3. If  $c \geq n$  then  $c \leftarrow c - n$
4. Return  $(c)$ .

Ex. 6 at 2:14–33.

105. “In Montgomery reduction, the value  $\mu$  is used to zero  $w$  least significant bits of a value  $a$ ,” whereby “[f]irst, a multiplier  $m = \mu a \bmod 2^w$  is computed,” where “[t]he value  $m$  has at most  $w$  bits.” Ex. 6 at 2:47–53. “Adding  $a + mn$  will zero  $w$  least significant bits of  $a$ , and  $a$  may be shifted down  $w$  bits.” *Id.* “Since typically  $L = kw$ , where  $k$  is the number of  $w$ -bit words in  $R$ [,] this operation is repeated  $k$  times to effect the Montgomery reduction  $aR^{-1} \bmod n$ .” *Id.*

106. The patent teaches that “efficiency may be increased by pre-computing certain fixed values to be used in the calculations,” where “[s]uch values include  $\mu = (-n)^{-1} \bmod 2^w$ , for

some  $w$  typically being the bit size of a word (or block) of the value (or perhaps the entire value) being operated on; and  $R^2 \bmod n$ .” Ex. 6 at 2:34–46.

107. The patent further teaches that “[i]n a register-based processor, registers are typically used to hold components of the value to be reduced, namely the precomputed value  $\mu$  and the modulus  $n$ .” Ex. 6 at 2:59–61.

108. The inventors recognized these technological problems and discovered improvements in modular reduction engines for computers (*e.g.*, Montgomery engines) to address them. *See, e.g.*, Ex. 6 at 3:21–45, 5:28–36, 3:40–45, 5:24–35, 5:45–6:19, 6:51–65.

109. For example, the patent teaches techniques for performing, on a cryptographic apparatus, a Montgomery-style reduction in a cryptographic operation that includes obtaining an operand for the cryptographic operation; computing a modified operand using a reduction value, instead of a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, where the reduction value is a function of the modulus; and outputting the modified operand. *See, e.g.*, Ex. 6 at 4:40–6:65. The patent teaches that such inventive techniques can reduce the number of multiplications and registers needed to effect the modular reduction, thereby providing a new and inventive technique for efficient modular reduction machines.<sup>116</sup> *See, e.g., id.* at 3:40–42, 5:28–36, 6:2–19, 6:51–65. For example, the patent teaches that “[i]n a machine 22 that has a limited number of registers and/or computational capabilities, it is desirable to reduce both the number of stored values and the number of computations,” and that “[t]o avoid having to store

---

<sup>116</sup> A register is hardware in a CPU for temporary storage of data during program execution. *See, e.g.*, <https://techterms.com/definition/register>; <https://www.allaboutcircuits.com/video-lectures/internal-registers-alu/>; <https://gunkies.org/wiki/Register>; <https://www.theiotacademy.co/blog/registers-in-cpu/>.

both  $\mu$  and  $n$ , it has been recognized by the inventor that a modified reduction value or a logical shift or signed version of such a value can be used in place of  $\mu$  and  $n$  for the bulk of the low-order reduction.” *Id.* at 5:28–36. The patent also teaches that the inventive technique “avoids both the multiplication necessary to compute  $m$  and the storage required for  $\mu$ ” and that the modified reduction value “does not require more registers than would be needed” otherwise. *Id.* at 6:2–19. The patent further teaches that the inventors observed significant benefits of the inventive techniques when used, for example, to perform ECC operations using resource-constrained computer processor architectures (e.g., “the popular ARM architecture”). *Id.* at 6:51–65.

\* \* \*

110. Malikie made multiple attempts to contact MARA regarding Malikie’s patent portfolio and to engage in licensing discussions. Malikie sent a first letter to MARA on March 28, 2025, which identified exemplary patents (including several of the Asserted Patents) and MARA services that infringe them. Malikie conveyed its intent to offer a license to MARA and its desire to begin patent licensing discussions. MARA did not respond. Malikie sent a second letter on April 18, 2025, which identified additional patents (including the remaining Asserted Patents) and infringing MARA services. Malikie reiterated its intent to offer MARA a license and its desire to schedule a meeting to discuss the issue further. MARA did not respond to that letter either.

111. Given MARA’s refusal to respond to Malikie’s attempts to engage in licensing discussions, Malikie believes it has no recourse but to file this action to seek just compensation for and, where appropriate, injunctive relief from MARA’s unauthorized use of Malikie’s patents.

### **JURISDICTION AND VENUE**

112. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.



113. This civil action arises under the patent laws of the United States, 35 U.S.C. § 1 *et seq.*, including without limitation 35 U.S.C. §§ 271, 281, 283, 284, and 285. This is a patent infringement lawsuit over which this Court has subject matter jurisdiction under, *inter alia*, 28 U.S.C. §§ 1331, 1332, and 1338(a).

114. This District has general and specific personal jurisdiction over Defendant because, directly or through intermediaries, Defendant has committed acts within this District giving rise to this action; is present in and transacts and conducts business, directly, and/or indirectly, in this District and the State of Texas; and transacts and conducts business with residents of this District and the State of Texas.

115. Plaintiffs' causes of action arise, at least in part, from Defendant's contacts with and activities in and/or directed at this District and the State of Texas. For example, MARA owns and/or operates bitcoin mining facilities in this Judicial District, including in McCamey, Texas (Upton County) and Hearne, Texas (Robertson County).<sup>117</sup> MARA also owns and/or operates bitcoin mining facilities in Garden City, Texas; Granbury, Texas; and Hansford County, Texas.<sup>118</sup> MARA has also purposefully availed itself of the laws of the State of Texas. For example, on information and belief, MARA has located bitcoin mining facilities in Texas, which in part give rise to this action, because MARA perceives the State of Texas as a "generally favorable regulatory environments for bitcoin miners compared to other states." MARA 2025 10-K at 12.

116. MARA is also a member of the Texas Blockchain Council, an "industry association working to make the State of Texas the jurisdiction of choice for bitcoin, blockchain, and digital

---

<sup>117</sup> See <https://www.mara.com/operations>; <https://www.mara.com/posts/mara-announces-25-megawatt-micro-data-center-project-powered-by-excess-natural-gas-from-oilfields>; MARA 2025 10-K at 10-11.

<sup>118</sup> *Id.*; <https://ir.mara.com/news-events/press-releases/detail/1389/mara-holdings-announces-closing-of-texas-wind-farm-acquisition>.

asset innovation.”<sup>119</sup> According to the Texas Blockchain Council, it “promote[s] blockchain technology initiatives such as bitcoin mining that drive growth and benefit the citizens of Texas” and “exist[s] to amalgamate the influence of our members, to advocate for blockchain-centric public policy initiatives and to educate members of government about the benefits of blockchain technology.”<sup>120</sup> The Texas Blockchain Council works to influence the state of the law in Texas as it relates to bitcoin, blockchain, and digital assets.<sup>121</sup>

117. Defendant has infringed the Asserted Patents within this District and the State of Texas by making, using, selling, offering for sale, and/or importing or by having made, used, sold, offered for sale, and/or imported in or into this District and elsewhere in the State of Texas, products and services covered by claims in the Asserted Patents, including without limitation products that, when made or used, practice the claimed methods of the Asserted Patents. Defendant, directly and through intermediaries, has and continues to make, use, sell, offer for sale, import, ship, distribute, advertise, promote, and/or otherwise commercialize such infringing products and services in or into this District and the State of Texas. Defendant regularly conducts and solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from goods and services provided to residents of this District and the State of Texas.

---

<sup>119</sup> <https://texasblockchaincouncil.org/about>; <https://texasblockchaincouncil.org/membership> (identifying MARA as an Executive Partner)

<sup>120</sup> <https://texasblockchaincouncil.org/>.

<sup>121</sup> See, e.g., <https://texasblockchaincouncil.org/policy-page> (“The Texas Blockchain Council is a proud member of the Texas Innovation and Technology Caucus. Our members are actively working to provide subject matter expertise to this group of forward-thinking legislators with a focus on the following policy initiatives.”); <https://www.itcaucus.com/> (“Members of the Texas House of Representatives and Texas Senate formed the bipartisan Innovation and Technology Caucus of the Texas Legislature (IT Caucus) as a policy shop and industry partner to focus on educating and informing members on ways to further advance technology industry innovation, growth, and competitiveness here in Texas, and strengthening the already significant impact this sector has on the state’s economy.”).

118. This Court has personal jurisdiction over Defendants pursuant to TEX. CIV. PRAC. & REM. CODE § 17.041 *et seq.*

119. Venue is proper in this District under 28 U.S.C. §§ 1391(b)-(c) and 1400(b).

120. Defendant is doing business, either directly or through respective agents, on an ongoing basis in this Judicial District and elsewhere in the United States, and has committed and continues to commit acts of infringement in this district. MARA Holdings, Inc. has regular and established places of business in this Judicial District, including in McCamey, Texas (Upton County) and Hearne, Texas (Robertson County), where MARA owns and/or operates bitcoin mining facilities. On information and belief, Defendant has and continues to make, use, sell, offer to sell, and/or import infringing products and services into and/or within this District, maintains a permanent and/or continuing presence within this District, and has the requisite minimum contacts with this District such that this venue is a fair and reasonable one. Upon information and belief, Defendant has transacted and, at the time of the filing of the Complaint and this First Amended Complaint, is continuing to transact business within this District.

### **FIRST CLAIM**

#### **(Infringement of the '827 Patent)**

121. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

122. The '827 Patent is generally directed to improved techniques for use in cryptographic algorithms, and, in particular, to methods and apparatuses for generating a public key of the signer of a digital signature by computing  $Q=r^{-1}(sR-eG)$ , where G comprises a generator of an elliptic curve group that includes a first elliptic curve point R and a second elliptic curve point Q.

123. Defendant has been on notice of the '827 Patent and a specific factual basis for its infringement of the '827 Patent since at least March 28, 2025. On information and belief, Defendant did not take any action to stop its infringement.

124. Defendant has, under 35 U.S.C. § 271(a), directly infringed, and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including without limitation at least claim 1 of the '827 Patent, by making, using, testing, selling, offering for sale, and/or importing hardware and/or software including devices and software that comply with the Bitcoin protocol (excluding any products licensed under the '827 Patent), such as bitcoin mining equipment (including, for example, hardware and software for digital asset mining, including mining rigs, application-specific integrated circuits (ASICs), computers, nodes, miners, and software applications) and wallets (including hardware and software that functions as a bitcoin wallet). An exemplary claim chart showing one way in which MARA infringes claim 1 of the '827 Patent is attached as Exhibit 7.

125. Defendant's infringement has been and continues to be willful in view of the above and its failure to take any action, even after being put on notice, to stop its infringement.

## **SECOND CLAIM**

### **(Infringement of the '370 Patent)**

126. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

127. The '370 Patent is generally directed to improved techniques for use in cryptographic algorithms, and, in particular, to methods and apparatuses for verifying a digital signature included with a message using a public key omitted from the message but recovered by computing  $Q=r^{-1}(sR-eG)$ , where  $G$  comprises a generator of an elliptic curve group that includes

the elliptic curve point R and the elliptic curve point Q, and wherein e is a hash value computed from the electronic message M.

128. Defendant has been on notice of the '370 Patent and a specific factual basis for its infringement of the '370 Patent since at least March 28, 2025. On information and belief, Defendant did not take any action to stop its infringement.

129. Defendant has, under 35 U.S.C. § 271(a), directly infringed, and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including without limitation at least claim 1 of the '370 Patent, by making, using, testing, selling, offering for sale, and/or importing hardware and/or software including devices and software that comply with the Bitcoin protocol (excluding any products licensed under the '370 Patent), such as bitcoin mining equipment (including, for example, hardware and software for digital asset mining, including mining rigs, application-specific integrated circuits (ASICs), computers, nodes, miners, and software applications) and wallets (including hardware and software that functions as a bitcoin wallet). An exemplary claim chart concerning one way in which MARA infringes claim 1 of the '370 Patent is attached as Exhibit 8.

130. Defendant's infringement has been and continues to be willful in view of the above and its failure to take any action, even after being put on notice, to stop its infringement.

### **THIRD CLAIM**

#### **(Infringement of the '960 Patent)**

131. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

132. The '960 Patent is generally directed to finite field engines and methods for use with cryptographic systems, and, in particular, techniques that enable the performance of finite

field operations on elements of a finite that include, among other things, representing each finite field element as a predetermined number of machine words, performing a non-reducing wordsized finite field operation on the representations and completing the operation for each word to obtain an unreduced result, performing a specific modular reduction of the unreduced result to reduce it to that of a field element, and using the reduced result in a cryptographic operation.

133. Defendant has been on notice of the '960 Patent and a specific factual basis for its infringement of the '960 Patent since at least March 28, 2025.

134. Defendant has, under 35 U.S.C. § 271(a), directly infringed, literally and/or under the doctrine of equivalents, one or more claims, including without limitation at least claim 3 of the '960 Patent, by having made, used, tested, sold, offered for sale, and/or imported hardware and/or software including devices and software that complied with the Bitcoin protocol (excluding any products licensed under the '960 Patent), such as bitcoin mining equipment (including, for example, hardware and software for digital asset mining, including mining rigs, application-specific integrated circuits (ASICs), computers, nodes, miners, and software applications) and wallets (including hardware and software that functions as a bitcoin wallet). An exemplary claim chart showing one way in which MARA infringed claim 3 of the '960 Patent is attached as Exhibit 9.

#### **FOURTH CLAIM**

##### **(Infringement of the '062 Patent)**

135. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

136. The '062 Patent is generally directed to finite field engines and methods for use with cryptographic systems, and, in particular, techniques that enable the performance of finite

field operations on elements of a finite field that include, among other things, obtaining a first set of instructions for performing the finite field operation on values representing the elements of the finite field and executing it to generate an unreduced result, obtaining a second set of instructions for performing a modular reduction for a specific finite field and executing it to generate a reduced result, and providing the reduced result as an output for use in a cryptographic operation.

137. Defendant has been on notice of the '062 Patent and a specific factual basis for its infringement of the '062 Patent since at least March 28, 2025.

138. Defendant has, under 35 U.S.C. § 271(a), directly infringed, literally and/or under the doctrine of equivalents, one or more claims, including without limitation at least claim 3 of the '960 Patent, by having made, used, tested, sold, offered for sale, and/or imported hardware and/or software including devices and software that complied with the Bitcoin protocol (excluding any products licensed under the '062 Patent), such as bitcoin mining equipment (including, for example, hardware and software for digital asset mining, including mining rigs, application-specific integrated circuits (ASICs), computers, nodes, miners, and software applications) and wallets (including hardware and software that functions as a bitcoin wallet). An exemplary claim chart showing one way in which MARA infringed claim 1 of the '062 Patent is attached as Exhibit 10.

## **FIFTH CLAIM**

### **(Infringement of the '961 Patent)**

139. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

140. The '961 Patent is generally directed to key generation within public key cryptosystems, and, in particular, techniques for generating a key  $k$  for use in a cryptographic

function performed over a group of order  $q$  that include, for example, generating a seed value  $SV$  from a random number generator, performing a hash function  $H()$  on the seed value  $SV$  to provide an output  $H(SV)$ , determining whether the output  $H(SV)$  is less than the order  $q$  prior to reducing mod  $q$ , accepting the output  $H(SV)$  for use as the key  $k$  if the value of the output  $H(SV)$  is less than the order  $q$ , rejecting the output  $H(SV)$  as the key if the value is not less than the order  $q$ , repeating the preceding steps if the output  $H(SV)$  is rejected, and providing the key  $k$  for use in performing the cryptographic function if the output  $H(SV)$  is accepted, wherein the key  $k$  is equal to the output  $H(SV)$ .

141. Defendant has been on notice of the '961 Patent and a specific factual basis for its infringement of the '961 Patent since at least April 18, 2025.

142. Defendant has, under 35 U.S.C. § 271(a), directly infringed, literally and/or under the doctrine of equivalents, one or more claims, including without limitation at least claim 1 of the '961 Patent, by having made, used, tested, sold, offered for sale, and/or imported hardware and/or software including devices and software that complied with the Bitcoin protocol (excluding any products licensed under the '961 Patent), such as bitcoin mining equipment (including, for example, hardware and software for digital asset mining, including mining rigs, application-specific integrated circuits (ASICs), computers, nodes, miners, and software applications) and wallets (including hardware and software that functions as a bitcoin wallet). An exemplary claim chart showing one way in which MARA infringed claim 1 of the '961 Patent is attached as Exhibit 11.



**SIXTH CLAIM**

**(Infringement of the '286 Patent)**

143. Plaintiffs incorporate by reference the preceding paragraphs of this First Amended Complaint.

144. The '286 Patent is generally directed to systems and methods for reducing the computation and storage requirements for a Montgomery style reduction and, in particular, to techniques for performing, on a cryptographic apparatus, a Montgomery-style reduction in a cryptographic operation that includes obtaining an operand for the cryptographic operation; computing a modified operand using a reduction value, instead of a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than per form a cancellation thereof, where the reduction value is a function of the modulus; and outputting the modified operand.

145. Defendant has been on notice of the '286 Patent since at least March 28, 2025, and a specific factual basis for its infringement of the '286 Patent since at least April 18, 2025. On information and belief, Defendant did not take any action to stop its infringement.

146. Defendant has, under 35 U.S.C. § 271(a), directly infringed, and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including without limitation at least claim 1 of the '286 Patent, by making, using, testing, selling, offering for sale, and/or importing hardware and/or software including devices and software that comply with the Bitcoin protocol (excluding any products licensed under the '286 Patent), such as bitcoin mining equipment (including, for example, hardware and software for digital asset mining, including mining rigs, application-specific integrated circuits (ASICs), computers, nodes, miners, and software applications) and wallets (including hardware and software that functions as a bitcoin

wallet). An exemplary claim chart showing one way in which MARA infringes claim 1 of the '286 Patent is attached as Exhibit 12.

147. Defendant's infringement has been and continues to be willful in view of the above and its failure to take any action, even after being put on notice, to stop its infringement.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs pray for judgment against MARA as follows:

148. That MARA has infringed each of the Asserted Patents and will continue to infringe the '827 Patent, '370 Patent, and '286 Patent;

A. That MARA's infringement of the '827 Patent, '370 Patent, and '286 Patent have been willful;

B. That MARA pay Plaintiffs damages adequate to compensate for its past infringement of each of the Asserted Patents, and present and future infringement of the '827 Patent, '370 Patent, and '286 Patent, together with interest and costs under 35 U.S.C. § 284;

C. That MARA pay prejudgment and post-judgment interest on the damages assessed;

D. That MARA pay Plaintiffs enhanced damages pursuant to 35 U.S.C. § 284;

E. That MARA be enjoined from infringing the '827 Patent, '370 Patent, and '286 Patent, or if its infringement is not enjoined, that MARA be ordered to pay ongoing royalties to Plaintiffs for any post-judgment infringement of the '827 Patent, '370 Patent, and '286 Patent;

F. That this is an exceptional case under 35 U.S.C. § 285; and that MARA pay Plaintiffs' attorneys' fees and costs in this action; and

G. That Plaintiffs be awarded such other and further relief, including equitable relief, as this Court deems just and proper.

**DEMAND FOR JURY TRIAL**

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs hereby demands a trial by jury on all issues triable to a jury.

Respectfully submitted,

/s/ Khue v. Hoang

Khue V. Hoang  
Reichman Jorgensen Lehman & Feldberg LLP  
400 Madison Avenue, Suite 14D  
New York, NY 10017  
Tel: (212) 381-1965  
[khoang@reichmanjorgensen.com](mailto:khoang@reichmanjorgensen.com)

Matthew G. Berkowitz  
Reichman Jorgensen Lehman & Feldberg LLP  
100 Marine Parkway, Suite 300  
Redwood Shores, CA 94065  
Tel: (650) 623-1401  
[mberkowitz@reichmanjorgensen.com](mailto:mberkowitz@reichmanjorgensen.com)

Philip J. Ekle  
Reichman Jorgensen Lehman & Feldberg LLP  
1909 K Street, NW, Suite 800  
Washington, DC 20006  
Tel: (202) 894-7310  
[peklem@reichmanjorgensen.com](mailto:peklem@reichmanjorgensen.com)

*Of Counsel:*

Mark D. Siegmund  
TX Bar No. 24117055  
Cherry Johnson Siegmund James, PC  
7901 Fish Pond Rd., 2nd Floor  
Waco, TX 76710  
Telephone: (254) 732-2242  
Facsimile: (866) 627-3509  
Email: [msiegmund@cjsjlaw.com](mailto:msiegmund@cjsjlaw.com)

*Attorneys for Plaintiffs Malikie Innovations Ltd.  
and Key Patent Innovations Ltd.*

**CERTIFICATE OF SERVICE**

The undersigned does hereby certify that a true and correct copy of the foregoing document was served on all counsel of record via the Court's electronic filing system in accordance with the Federal Rules of Civil Procedure and the Local Rules of the Western District of Texas on this 25<sup>th</sup> day of July 2025.

/s/ Mark D. Siegmund  
Mark D. Siegmund